

Loi sur la protection des données : la situation du canton de Berne

Autor(en): **Siegenthaler, Markus**

Objektyp: **Article**

Zeitschrift: **Les intérêts de nos régions : bulletin de l'Association pour la défense des intérêts jurassiens**

Band (Jahr): **66 (1995)**

Heft 4

PDF erstellt am: **13.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-824400>

Nutzungsbedingungen

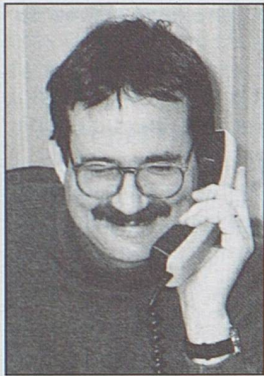
Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.



par Markus Siegenthaler, Délégué à la protection des données du canton de Berne

Loi sur la protection des données

La situation du canton de Berne

La nouvelle Constitution du canton de Berne, datée du 6 juin 1993, est entrée en vigueur le 1^{er} janvier 1995. Son article 18 prévoit un droit à la protection des données.

La loi bernoise sur la protection des données remonte, comme la loi jurassienne, à 1986. Elle est entrée en application le 1^{er} janvier 1988.

Dans les autres textes législatifs, le droit bernois ne connaît ni décret ni ordonnance sur la protection des données.

Le décret d'organisation de la Direction de la justice, des affaires communales et des affaires ecclésiastiques précise l'organisation du Bureau pour la surveillance de la protection des données. De nombreux textes spéciaux contiennent des dispositions régissant la protection des données, comme le décret sur les droits et les devoirs de patients, l'ordonnance sur l'engagement par la police d'enregistreurs d'images et de sons lors de manifestations de masse, ou les textes législatifs de procédure prévoyant des réglementations spéciales sur les données relatives à des procédures classées, comme l'ordonnance sur le régime applicable aux mineurs délinquants.

La loi fédérale comme la loi jurassienne sur la protection des données concordent avec la loi bernoise sur les questions fondamentales. Les différences existant entre elles portent sur des questions de détail.

Il faut mentionner notamment le fait que, contrairement à la loi fédérale, la loi bernoise ne contient pas de disposition sur les profils de personnalité. Elle ne prévoit pas non plus de réglementation directement applicable sur les procédures d'appel électroniques. Contrairement aux lois fédérale et jurassienne, la loi bernoise ne règle pas le transfert de données à

l'étranger. Comme la loi jurassienne, la loi bernoise n'est pas applicable dans le cadre d'une procédure administrative de première instance (à la différence de la loi fédérale).

Organisation

a) Comparaison entre Confédération, canton du Jura et canton de Berne. Comme on l'a vu dans l'article précédent (C. Grand), la Confédération dispose d'une Commission de la protection des données et d'un Préposé à la protection des données. La Commission est une autorité judiciaire, c'est-à-dire qu'elle peut être appelée à trancher dans les recours contre les décisions de l'administration. Le Préposé à la protection des données n'est pas une personne, comme dans le canton de Berne, mais un service administratif employant quelque douze personnes (toutes n'exercent pas cette fonction à titre principal).

Le canton du Jura a pour ainsi dire repris une moitié de la solution fédérale. La commission y est à la fois autorité de surveillance et autorité de justice administrative. Dans le canton de Berne en revanche, il n'existe qu'un délégué à la protection des données, qui ne remplit aucune fonction de justice administrative d'importance.

b) Le délégué bernois à la protection des données. C'est le Conseil exécutif qui nomme le délégué bernois à la protection des données. Du point de vue matériel, le délégué à la protection des données est totalement indépendant ; il n'est pas subordonné au Conseil exécutif. Du point de vue administratif, il est rattaché à l'Office juridique de la Direction de la justice, des affaires communales et des affaires ecclésiastiques. Dans les faits, le délégué à la protection des données est un service qui occupe une seule personne. Le coordinateur des affaires législatives est son suppléant. Le pool de secrétaires du secrétariat général de la Direction de la justice, des affaires communales et des affaires ecclésiastiques lui fournit l'infrastructure dont il a besoin. Il ne dispose d'aucune ressource dans le domaine informatique.

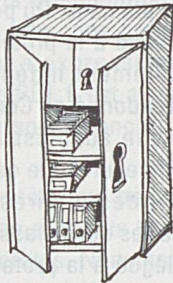
La loi sur l'information du public : quels sont les changements apportés ?

Après les articles de Mme Grand et de M. Moritz, il n'y aurait plus grand-chose à dire, si la loi sur l'information et son ordonnance n'étaient pas entrées en vigueur le 1^{er} janvier 1995, en même temps que la nouvelle Constitution, qui crée un droit constitutionnel d'être informé.



Ces deux dessins montrent les changements apportés par la législation sur l'information : les deux armoires contiennent les données personnelles qui se trouvent dans une commune. L'armoire du dessus a les portes fermées. Elle illustre la situation juridique telle qu'elle se présentait avant l'entrée en vigueur de la législation sur l'information. Le trou de serrure de taille disproportionnée montre qu'un particulier avait déjà la possibilité, alors, de consulter des données personnelles se trouvant dans une commune, comme par exemple des renseignements tirés du contrôle des habitants, des données du registre fiscal, des données nécessaires à des travaux de recherche ou encore des données concernant une personne ayant accepté leur communication.

L'armoire dont les portes sont ouvertes, illustre l'état actuel des choses. Elle compte trois casiers. Supposons que le dernier contient les dossiers personnels, celui du milieu le registre des propriétaires de chiens et celui du dessus le registre des habitants et le registre fiscal. Les portes de l'armoire ne sont pas grand ouvertes. Pourquoi ? La loi sur l'information du public prévoit que la consultation de dossiers par un tiers peut être contraire aux intérêts dignes de protection de la personne mentionnée dans le dossier. «Intérêts dignes de protection» est une notion juridique imprécise. Dans le langage courant, on parle de notion Deux exemples à ce propos :



a) Supposons qu'un revendeur d'adresses cherche à consulter un fichier de personnel pour savoir adresser aux hauts fonctionnaires disposant d'un revenu donné une publicité pour une voiture. Certains de ces fonctionnaires auront sûrement collé depuis longtemps un autocollant «Pas de publicité» sur leur boîte aux lettres et fait apposer un asté-

risque à côté de leur nom dans l'annuaire téléphonique. L'intérêt de ces fonctionnaires à ne pas recevoir de publicité passe avant l'intérêt du revendeur à connaître leurs adresses à des fins publicitaires. Le revendeur devra attendre derrière les portes à demi ouvertes de l'armoire et ne pourra regarder dedans.

b) Il en va autrement lorsqu'un journaliste cherche à consulter le même fichier pour écrire un article sur la pratique des communes en matière de classification. On peut imaginer que les fonctionnaires se défendront contre la publication de leur salaire en invoquant le fait qu'elle pourrait engendrer envie et malveillance. Cet intérêt ne passera pas avant celui du journaliste : qui est payé par le public devra accepter de voir ce même public contrôler si les principes qui régissent les salaires des fonctionnaires sont acceptables.

Dans la partie supérieure de l'armoire, on aperçoit un petit coffre fermé. Que renferme-t-il ? Les données particulièrement dignes de protection au sens de l'art. 3 de la LPD (l'encadré ci-contre les énumère). Restons-en pour le moment aux données personnelles. Si un secrétaire communal précise dans sa lettre de candidature à quel parti politique et à quelle Église il appartient, ces deux informations sont des données dignes de protection (opinion et appartenance politiques et religieuses) qui relèvent donc du petit coffre. Si le même secrétaire communal cherche, au cours de sa carrière, à remplacer la moquette de son bureau par du parquet, parce qu'il est allergique à la poussière, et joint à sa demande un certificat médical pour la justifier, il communique des informations sur son état de santé. Ce certificat médical a lui aussi sa place dans le petit coffre. Ainsi, une même lettre (candidature) peut contenir des données accessibles et d'autres, qui devraient être découpées aux ciseaux et mises sous clef.

La deuxième catégorie de données destinées au petit coffre sont celles qui doivent obligatoirement, d'entrée de jeu, être gardées secrètes. Parmi celles-ci, on trouve le secret fiscal au sens de la loi sur les impôts et l'obligation de discrétion au sens de la loi sur les oeuvres sociales. Il est intéressant de noter qu'un décompte de traitement, en principe accessible dès qu'il est dressé par le service du per-

Données particulièrement dignes de protection

Art. 3 Est considérée comme donnée particulièrement digne de protection toute information relative

- aux opinions, appartenances et activités religieuses, philosophiques ou politiques ainsi qu'à l'appartenance raciale ;
- à la sphère intime de la personne, en particulier à son état psychique, mental ou physique ;
- aux mesures d'aide sociale ou d'assistance ;
- aux enquêtes de la police, aux procédures pénales, aux infractions ainsi qu'aux peines et mesures qui les ont sanctionnées.

sonnel d'une commune, ne peut plus être communiqué dès qu'il a été soumis aux autorités fiscales dans le cadre de la procédure de taxation.

La communication à des particuliers d'informations concernant d'autres particuliers est désormais réglée dans une procédure décisionnelle. Une commune doit, en principe, procéder de manière identique pour répondre à la demande de renseignements d'un particulier ou à une demande de permis de construire. Supposons qu'un fabricant de nourriture pour chiens cherche à avoir, à des fins publicitaires, la liste des propriétaires de chiens. Jusqu'à présent, la commune répondait par la négative (quand elle réagissait correctement). Il arrivait qu'elle réponde par l'affirmative (quand elle ne réagissait pas correctement). Mais elle ne rendait pas de décisions. Le fabricant de nourriture ne pouvait faire recours contre une réponse négative auprès de la préfecture et, de son côté, le propriétaire de chien n'avait aucune possibilité de se défendre. Il en va autrement aujourd'hui et le maniement des informations revêt une nouvelle tournure.

La pratique

a) Le blocage des données. L'art. 13 de la LPD (voir encadré) est un instrument connu. Jusqu'ici, il était surtout utilisé lorsqu'un contribuable voulait se faire rayer du registre fiscal, que la commune est libre de vendre. Il justifiait généralement son attitude par les mots d'envie et de malveillance. Pareilles demandes

étaient pratiquement toutes acceptées sans exception. De plus, il est très simple de demander un blocage : une carte postale suffit. Le blocage de données ne garantit pas leur protection absolue. Dans l'ancien droit, il est arrivé que des personnes qui ne payaient pas régulièrement leurs factures demandent le blocage de leurs données au moment de quitter leur commune de domicile, de façon à ce que les créanciers ne puissent connaître leur nouvelle adresse. Ces blocages abusifs pouvaient être levés. Dans le nouveau droit, le blocage de données joue un rôle important, même s'il est limité.

b) Le droit d'être entendu. La personne qui a demandé le blocage de ses données a la garantie de pouvoir donner son avis lorsqu'un particulier cherche à se renseigner à son sujet. A la différence de la procédure d'octroi d'un permis de construire, l'intéressé n'est pas entendu dans le cas normal. Il ne l'est que si le secrétaire communal soupçonne qu'il s'agit là de données dignes de protection ou d'intérêts privés prépondérants. Le secrétaire communal a parfois là une tâche difficile à remplir : supposons qu'un inconnu, qui n'a pas à indiquer ses motifs, demande à avoir la liste de tous les élèves de la commune. Si cette personne envisage – ce que le secrétaire n'est pas censé savoir – d'acquérir de nouveaux membres pour un club sportif, il n'y a pas matière à douter. Mais que doit répondre le secrétaire communal si des parents ont signalé que leur fille, en âge de scolarité a un long trajet à faire pour aller à l'école, traverse une forêt et

a peur qu'il lui arrive quelque chose, qu'un inconnu parvienne à trouver son adresse et, éventuellement son horaire de cours ? Il devrait être de mise de douter au sens où l'entend l'article 14 de l'ordonnance sur l'information, surtout au cours des mois à venir.

En résumé, on peut dire que l'entrée en vigueur, dans le canton de Berne, de la législation sur l'information a placé le sort de la protection des données dans les mains des personnes intéressées : si celles-ci approuvent cette législation libérale, elles n'ont rien à faire. Dans le cas contraire, elles doivent exiger le blocage de leurs données personnelles dans tous les services disposant d'information les concernant.

Dispositions régissant les aspects techniques

Il faut commencer par prendre l'article 17 de la loi sur la protection des données. A la différence du droit fédéral, le droit cantonal ne concrétise pas ses dispositions dans une ordonnance. A l'intérieur du canton, c'est l'arrêté du Conseil exécutif no 4637 du 9 décembre 1992 qui concrétise l'article 17 (pas pour les communes, toutefois). Cet arrêté donne aux services cantonaux un certain délai pour classer leurs applications informatiques en trois catégories. Il définit ensuite les mesures de sécurité à prendre dans chaque catégorie.

L'ordonnance fédérale sur la protection des données (RS 235.11, en particulier les art. 8 à 12 et 20) n'est pas seulement utile à l'application du droit fédéral dans le canton, mais elle sert également à combler les lacunes du droit cantonal. Autre texte à utiliser (dans les mêmes conditions juridiques) : le guide édité par le Préposé fédéral à la protection des données concernant les mesures techniques et organisationnelles de la protection des données. Ces «normes» contiennent bien souvent l'indication selon laquelle il faut tenir compte du développement technique. Sans l'aide d'un informaticien, le juriste ne sera pas en mesure d'évaluer ce développement technique. En ce qui concerne l'application du droit fédéral par les cantons, les délégués cantonaux à la protection des données ont la possibilité de recourir aux services des informaticiens de la Confédération. Il est juste d'exiger au niveau cantonal ce que la Confédération exige. Il est évident, dans tous les cas de figure, que donner des connaissances d'informatique à un service cantonal de protection des données est loin d'être inutile.

La question de la responsabilité dans le domaine technique

Un article paru dans le numéro 4/94 de *BE-info* présente le point de vue de l'utilisateur. Plusieurs problèmes y sont soulevés :

Droit de blocage

Art. 13

¹Toute personne intéressée peut demander le blocage de ses données à condition qu'elle prouve un intérêt digne de protection.

²La communication est admissible malgré le blocage si

– l'autorité responsable y est contrainte par la loi ou si

– la personne intéressée abuse du droit.

³La personne intéressée peut demander le blocage de données au sens de l'article 12, 2^e alinéa et de leur communication réglée systématiquement en vertu de l'article 12, 3^e alinéa sans prouver qu'elle y trouve un intérêt digne de protection.



Chemins de fer du Jura

2726 Saignelégier

Tél. 039 51 18 25

2720 Tramelan

Tél. 032 97 40 06

Franches-Montagnes

Train +

◆ marche ou vélo

Train à vapeur

◆ Circulations les 14.5*

4.6*19.7*1.8*17.9*8.10

◆ Trains spx: sur demande

"Belle Epoque"

◆ Trains spx: sur demande

a) La responsabilité des applications informatiques est partagée : la tendance qui semble s'ensuivre est que chaque partie part du principe qu'elle n'est pas responsable, que la responsabilité est aux mains des deux parties. C'est le cas de l'utilisateur qui constate que les paramètres de son système sont mauvais, mais qui pense que la question relève de l'informaticien du service et de son chef. Cette hypothèse est de toute évidence fautive. Quel que soit le type de responsabilité qui entre en ligne de compte (responsabilité disciplinaire du fonctionnaire, responsabilité civile, responsabilité pénale), le simple fait pour une personne d'accepter l'éventualité des répercussions illégales de ses applications informatiques suffit pour engager sa responsabilité. Dans la pratique, il faut considérer cette disposition comme très importante.

b) Supérieurs hiérarchiques et utilisateurs s'estiment à la merci des informaticiens. Ils ont donc tendance à être mesurés dans leurs critiques, quand ils osent les exprimer. Le supérieur hiérarchique a là une fonction essentielle à remplir. C'est à lui de structurer son service de manière à institutionnaliser un dialogue entre informaticien et utilisateur, dialogue qui permette la critique. Il faut, en ce sens, instaurer une nouvelle « culture », tenant compte du fait que les systèmes informatiques ne peuvent, de par leur complexité, fonctionner sans erreur. A toutes les personnes concernées de réparer ces erreurs.

c) Le langage semble avoir un rôle central à jouer dans la perception de la responsabilité face aux applications informatiques. Le modèle est extrêmement simple : l'informaticien maîtrise aussi bien la langue technique de sa spécialité que la langue courante. L'utilisateur et son supérieur ne maîtrisent bien souvent que la langue courante. Il est donc logique, dans ces conditions, que soit utilisée la langue courante, accessible à tous, plutôt que la langue technique. Utilisateur et supérieur doivent se refuser obstinément à accepter des explications données par un informaticien dans une langue technique. L'article de M. Girardin (voir plus loin) montre bien qu'il est possible de présenter des processus techniques dans une langue accessible à tous.

Que doivent faire les communes ?

a) **Directement.** L'article 33, 1^{er} al. et l'article 37, 3^e al. de la LPD obligent toutes les corporations de droit communal (par exemple, les communes bourgeoises, les paroisses et les syndicats de communes, comme les syndicats hospitaliers) à créer leur propre autorité de surveillance de la protection des données et à définir les modalités de rapport en complétant le règlement de leur commune. Dans la plupart des cas, les communes ont chargé de cette fonction la commission de vérification des comptes, indépendante de l'administration. Elles sont libres de configurer leur service de protection des données comme elles l'entendent, en optant pour une personne ou pour un organe composé de représentants de l'administration et de personnes extérieures. La condition, dans cette deuxième option, est que les personnes extérieures soient majoritaires.

L'article 18 de la LPD oblige pour sa part les communes à tenir un registre des fichiers de données.

Dans la pratique, un grand nombre de services de protection des données ont été créés par modification du règlement communal. En revanche, la plupart des communes n'ont pas encore de registre des fichiers de données. Il est évident,

dans tous les cas de figure, que les services communaux de protection des données ont beaucoup de mal, sans moyens auxiliaires fournis par le canton (tels que listes de contrôle et autres), à s'acquitter de leurs travaux concrets. Le pendant de cet inconvénient majeur est que les autorités locales de surveillance sont mieux placées que les autorités centrales pour suivre sur place l'évolution des choses. Elles sont, par exemple, mieux informées des indiscretions éventuelles.

b) **Indirectement.** L'article 12 de la LPD n'autorise la communication de renseignements systématiques tirés du contrôle des habitants que si le règlement communal le prévoit expressément (depuis l'entrée en vigueur de la législation sur l'information, cela vaut également pour les renseignements systématiques tirés d'autres registres). Les partis politiques représentés sur place ne peuvent donc avoir connaissance chaque année de la liste des nouveaux électeurs que si le règlement le prévoit. Si la commune ne s'est pas dotée d'une réglementation, aucune liste ne peut être communiquée. Dans la pratique, deux variantes se sont imposées : la commune prévoit que des renseignements ne peuvent être communiqués sous forme de listes qu'à des fins idéales, ou elle permet globalement qu'ils le soient à des fins idéales et commerciales.

M O B I L I E R

C O N T E M P O R A I N

HADORN

MEUBLES HADORN SA 2740 MOUTIER

TEL. 032 93 43 31 FAX 032 93 59 42

Représentation de la situation du point de vue de la personne intéressée par un renseignement

Bureau d'encaissement, agence de publicité : quelques exemples concrets

Partons de l'hypothèse qu'un bureau d'encaissement est chargé, par un garagiste, d'exiger le paiement de quatre pneus impayés. Il faut signaler, d'emblée, que le garagiste a la possibilité, dans le canton de Berne, de se faire une idée générale de la fortune de son débiteur en consultant le registre fiscal public. Il n'existe pas de possibilité de blocage des renseignements tirés du registre fiscal.

Imaginons que le garagiste ne s'est adressé au bureau d'encaissement qu'après avoir reçu sa facture en retour avec la mention « destinataire inconnu ». Le bureau d'encaissement commencera par s'adresser au contrôle des habitants de l'ancienne commune de domicile. Dans une situation normale, la date du départ et la nouvelle commune de domicile seront connues. Si l'intéressé a fait bloquer les données le concernant, le bureau d'encaissement devra adresser une requête à la commune pour demander la levée de ce blocage. Généralement, une telle demande est justifiée par le fait que le blocage est abusif au sens de l'article 13 (2^e al., let. b) de la LPD. Dans la pratique, l'intéressé aura à se prononcer sur cette requête dans un délai de trois semaines. Passé ce délai,

la commune rendra une décision en l'espace d'une semaine environ. Généralement, elle lèvera le blocage. L'intéressé pourra faire recours contre cette décision auprès de la préfecture, et ce dans les trente jours. Le renseignement recherché ne sera fourni au bureau d'encaissement qu'à l'écoulement de ce délai de recours, c'est-à-dire huit semaines après le dépôt de la requête.

Autre exemple : une banque, désireuse d'inciter tous les adolescents âgés de 16 ans résidant dans une commune donnée à ouvrir leur propre compte en banque, ne pourra recevoir la liste de leurs adresses que si le règlement communal prévoit la communication de listes à des fins commerciales. Si le droit communal ne contient aucune disposition expresse ou ne prévoit la communication de listes qu'à des fins idéales, il sera impossible à la banque d'obtenir les adresses souhaitées. S'il existe une base légale, la banque doit être consciente du fait qu'elle ne pourra pas recevoir les données concernant les personnes qui ont demandé un blocage. De tels

blocages ont une valeur absolue en matière de communication de listes et la banque n'a aucun moyen de les lever.

Précisons encore que les communes peuvent fixer des émoluments, aussi bien pour la communication de renseignements ponctuels que pour la fourniture de listes.

La législation sur l'information du public nous a enseigné que la protection des données est elle aussi une notion changeante. Parce qu'elle représente quelque chose de nouveau, il est important d'en suivre les répercussions pratiques sur les personnes intéressées et de corriger les réglementations dont les résultats ne sont pas ou ne sont plus satisfaisants. Dans ce sens, la protection des données ne doit en aucun cas s'acharner à défendre des principes théoriques, mais elle doit chercher à résoudre de manière pragmatique les problèmes pratiques qui se posent aux individus dans la société informatisée qui est désormais la nôtre. ■

Une date à retenir :

jeudi 14 mars 1996 à 18 h. 30

à Moutier

Assemblée générale de l'ADIJ

Vos imprimés de A à Z avec un seul partenaire!

NOUVEAU

Nous réalisons
aussi
vos photolithos
en couleur.



IMPRIMERIE DU DÉMOCRATE SA

6, route de Courroux - 2800 Delémont - Tél. 066 22 17 51 - Fax 066 23 20 69