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

Herausgeber: Association pour la défense des intérêts jurassiens

Band: 66 (1995)

Heft: 4

Artikel: La loi jurassienne sur la protection des données à caractère personnel : ses implications juridiques pour les communes

Autor: Moritz, Jean

DOI: https://doi.org/10.5169/seals-824399

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 15.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

par Jean Moritz, Président de la Commission de la protection des données du Canton du Jura.

La loi jurassienne sur la protection des données à caractère personnel

Ses implications juridiques pour les communes

La loi jurassienne a été adoptée par le Parlement le 15 mai 1986. Elle est entrée en vigueur le 1er janvier 1987. Les communes avaient un délai de quatre ans pour adapter leur réglementation à la loi, délai durant lequel celle-ci ne leur était pas applicable.

La loi jurassienne, à l'instar des lois bernoise et valaisanne, s'inspire des solutions retenues par la loi modèle élaborée par la Conférence des directeurs cantonaux de Justice et Police. A l'époque, la loi jurassienne était considérée comme la plus complète et la plus détaillée (cf. Jean-Philippe Walter, *La protection de la personnalité lors du traitement de données à des fins statistiques*, page 264). Elle est considérée comme une loi moderne.

Les buts de la protection des données

Le but de la loi jurassienne est de protéger les droits fondamentaux, en particulier la personnalité, contre le traitement des données à caractère personnel (cf. art. premier). C'est particulièrement le droit au respect de la vie privée que la loi cherche à protéger. Ce droit est mentionné à l'art. 8 let. b de la Constitution jurassienne. Il figure également, et surtout, à l'art. 8 CEDH, qui stipule que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

Le droit au respect de la vie privée est un des aspects de la liberté personnelle.

La liberté personnelle est un droit constitutionnel fédéral non écrit, créé par la jurisprudence. Selon le Tribunal fédéral, elle est à la fois liberté centrale et principe directeur de l'ordre constitutionnel. Elle garantit : la liberté de mouvement, l'intégrité physique et psychique, les libertés élémentaires dont l'exercice est indispensable à l'épanouissement de la personne humaine. Elle est aussi considérée comme la condition permettant l'exercice des autres droits fondamentaux, en particulier ceux qui constituent les éléments indispensables de l'ordre démocratique dans un Etat fondé sur le droit (ATF 115 I a 268). Le droit au respect de la sphère privée est une de ces libertés élémentaires nécessaires à l'épanouissement de la personnalité, comme l'est le droit à la dignité, le droit à l'honneur, le libre arbitre (cf. Haller, in *Commentaire de la Constitution fédérale*, n. 82 ad liberté personnelle).

Pour la première fois, en 1987, le Tribunal fédéral a eu l'occasion de dire que la conservation de données strictement personnelles et non accessibles à chacun est susceptible de provoquer une atteinte à la liberté personnelle de l'individu concerné (cf. ATF 113 I a 257). En substance, le Tribunal fédéral retient «que quiconque prétend, avec quelque vraisemblance, que des renseignements personnels enregistrés à son sujet sont susceptibles de porter atteinte à sa liberté personnelle doit pouvoir en requérir la consultation sans avoir à justifier encore d'un autre intérêt digne de protection». Le droit constitutionnel confère, en effet, à la personne concernée le droit d'être renseignée, d'une part sur les données qui ont été enregistrées à son sujet par une autorité publique et, d'autre part, sur l'usage qui en a été fait. Le TF expose «que ce droit aux renseignements est appelé à jouer un rôle de plus en plus important pour la protection de l'individu, car le traitement informatique des données en permet la diffusion et le traitement immédiat à tous les échelons de l'administration publique».

Dans un arrêt plus récent (ATF 118 I b 277), le Tribunal fédéral rappelle que le droit de consulter un dossier (il s'agissait dans le cas d'espèce d'un dossier de police) est, certes, l'un des aspects du droit d'être entendu garanti par l'art. 4 CF,

mais il se trouve aussi en relation étroite avec la liberté personnelle et la protection de la vie privée et familiale, du domicile et de la correspondance au sens de l'art. 8 CEDH.

Les principes posés par le Tribunal fédéral sont repris et concrétisés par la loi jurassienne : à la section 2, elle définit les principes qui régissent le traitement de données à caractère personnel ; à la section 3, elle traite de la communication des données et en règle les modalités ; à la section 6, elle énumère les droits de la personne concernée.

Conditions matérielles auxquelles est subordonné le traitement des données à caractère personnel

Tout traitement de données à caractère personnel effectué par les pouvoirs publics doit être considéré comme une immixtion dans la sphère privée de la personne concernée, soit comme une atteinte à sa liberté personnelle, à sa «personnalité».

Ces «ingérences» sont admissibles aux conditions de l'art. 8 paragraphe 2 CEDH, d'une part ; elles sont, d'autre part, soumises aux conditions des articles 5 à 10 LPD.

Les articles 5, 6 et 8 définissent les conditions générales auxquelles est soumise l'admissibilité de toute restriction aux droits fondamentaux : une atteinte à un droit fondamental est autorisée dans la mesure où elle repose sur une base légale, si elle est justifiée par un intérêt public prépondérant et si elle respecte le principe de la proportionnalité (nécessité de l'atteinte, adéquation au but recherché). Un traitement qui ne serait pas justifié par un intérêt public prépondérant, qui ne reposerait sur aucune base légale ou qui serait inutile, respectivement impropre à atteindre le but visé, ne serait pas admissible.

Les articles 7, 9 et 10 qui posent les principes de la spécificité du but (principe de la finalité), de la véracité et de l'objectivité constituent les conditions spécifiques auxquelles est soumis le traitement de données à caractère personnel en tant que restriction à un droit fondamental.

Un traitement qui ne serait pas conçu dans un but déterminé à l'avance, qui reposerait sur des données inexactes, incomplètes, constituant un jugement de valeur sur la personne concernée ou qui donnerait une définition globale de son profil de personnalité serait illicite.

Champ d'application de la loi jurassienne

a) Champ d'application formel. La loi est applicable à l'Etat, au sens large (voir l'énumération de l'art. 3 al. 2 LPD) c'est-à-dire à tout organe ou personne qui dispose d'une part de la puissance publique cantonale, communale ou intercommunale, et cela indépendamment du droit appliqué, cantonal, communal ou fédéral. Ainsi, un traitement de données effectué par un organe cantonal en exécution du droit fédéral tombe sous le coup de la loi cantonale sur la protection des données.

Exceptions :

1. La loi jurassienne n'est pas applicable aux personnes privées et aux organes publics non cantonaux et non communaux.

2. Le Parlement et le Gouvernement sont exonérés de l'application de la loi, aux conditions de l'art. 24 LPD, c'est-à-dire lorsqu'ils traitent des données à caractère personnel dans le cadre de leurs activités respectives. Cette exemption doit être appréciée de manière restrictive. Ainsi, le Gouvernement n'est pas dans tous les cas à l'abri de la loi, selon la jurisprudence de la Commission cantonale de la protection des données (ci-après CPD). S'il peut, en vertu de son pouvoir de surveillance sur les fonctionnaires, dresser la liste de ceux qui accusent des arriérés d'impôts, il n'a pas le pouvoir de rendre une telle liste publique (RJJ 1994, p. 297 ss). Dans ce cas d'espèce, la CPD a posé clairement le principe que la liberté d'action du Gouvernement est limitée par les droits fondamentaux que la LPD tend à protéger.

b) Champ d'application matériel. La LPD s'applique à toutes les données, quelles que soient leur mode de traitement, les moyens et les procédés utilisés : manuels, informatiques, occasionnels, systématiques (cf. art. 3 al. 1 LPD).

Exceptions :

1. Elle n'est pas applicable au traitement de données effectué en situation de concurrence économique (cf. art. 22 LPD). Cette disposition vise les autorités ou les organes de l'Etat qui agissent comme des privés et qui sont soumis au droit privé. C'est le cas lorsqu'une activité de l'Etat ne poursuit pas directement une mission de service public. Ainsi, par exemple, lorsque l'Etat (ou une commune) gère ses immeubles, ses forêts ou

FMB

BUREAU D'INGENIEURS
PROJETS D'INSTALLATIONS ELECTRIQUES
HAUTE ET BASSE TENSION

ENTREPRISE GENERALE
VIABILISATION ELECTRIQUE, CONSTRUCTION D'INSTALLATIONS DE DISTRIBUTION MOYENNE TENSION POUR L'INDUSTRIE, ECLAIRAGE DE RUES, PLACES ET MONUMENTS

INSTALLATIONS ELECTRIQUES
INSTALLATIONS ELECTRIQUES A COURANT FORT ET FAIBLE

GESTION DES RESEAUX
RELEVES CADASTRAUX, PLANIFICATION ENERGETIQUE

TELEMATIQUE
INSTALLATION DE RESEAUX INFORMATIQUES INTEGRES

DELEMONT
Tél. (066) 21 31 31

PORRENTRUY
Tél. (066) 66 18 43

tout bien qui entre dans son patrimoine fiscal (par opposition au patrimoine administratif).

2. Le traitement de données à des fins scientifiques, statistiques et de planification ou de recherche échappe également à la loi, aux conditions de l'art. 25 LPD. Dans ce cadre, c'est le principe de l'anonymat qui prévaut.

Exemple : la CPD a fait interdiction au Service cantonal de l'aide sociale de communiquer à une personne privée (un universitaire) le fichier relatif aux bénéficiaires de l'aide au recouvrement des pensions alimentaires (ARPA). Elle a en revanche autorisé ledit service à procéder lui-même à l'envoi du questionnaire que l'universitaire en question souhaitait adresser aux bénéficiaires de l'ARPA et à en transmettre les réponses en retour à la requérante, après avoir écarté toute indication qui aurait pu permettre de déterminer l'identité des personnes concernées (cf. décision de la CPD du 25 novembre 1992).

3. La LPD n'est pas applicable aux procédures civiles, pénales et administratives pendantes, aux conditions de l'art. 23 LPD. L'exclusion du champ d'application de la LPD des procédures pendantes ne concerne toutefois que les données qui sont contenues dans un dossier de justice et pas, par exemple, les fichiers de la police qui constituent un dossier de police, quand bien même le dossier en cause concerne un prévenu. La CPD a ainsi autorisé un prévenu à consulter son dossier de police, malgré les procédures pénales pendantes à son encontre (décision de la CPD du 19 janvier 1994 en la cause S. contre commandant de la police cantonale jurassienne, publiée in RJJ, p. 13). Pour le surplus, il faut considérer que la consultation des données qui se trouvent dans un dossier de justice est régie par les lois de procédure qui priment la stricte application de la LPD, pour autant qu'elles assurent une protection équivalente.

Droit d'accès

Le droit d'accès est un droit fondamental. Celui-ci peut être restreint aux conditions posées à l'art. 34 LPD.

Suivant la jurisprudence du Tribunal fédéral citée au chapitre 2 ci-dessus, toute personne a le droit de connaître l'existence des fichiers qui la concernent. L'aménagement de ce droit est prévu à l'art. 32 LPD qui permet à toute personne d'avoir librement accès au catalogue et aux registres des fichiers. L'art. 33 lui permet, ensuite, de connaître le contenu des données qui la concernent et qui sont traitées dans un fichier déterminé.

Le libre accès au catalogue et aux registres et le droit d'accès au contenu des fichiers constituent les droits de base à défaut desquels la personne concernée ne serait pas en mesure d'exercer ses autres droits, à savoir celui de faire corriger les données inexactes (droit de rectification de l'art. 37), de faire suspendre toute communication de données à caractère personnel (art. 38), de faire interdire le traitement, de le faire cesser, de faire détruire les données déjà recueillies ou encore de faire constater l'illicéité du traitement (art. 36 LPD).

Les restrictions au droit d'accès sont celles qui justifient généralement une atteinte à un droit fondamental. Il y en a d'autres. Elles sont prévues à l'art. 34 al. 2, notamment la charge administrative disproportionnée qu'une demande de renseignements occasionnerait. Toutefois, le refus du droit à la communication des données en raison de la surcharge administrative qu'entraînerait le traitement de la requête ne peut être admis que très restrictivement. Cette circonstance ne constitue pas, en règle générale, une raison suffisante pour faire obstacle à l'exercice d'un droit juridiquement protégé (RJJ 1994, p. 14).

Les droits de procédure

Une personne qui s'estime lésée par un traitement illicite de données à caractère personnel peut intervenir auprès de l'autorité de surveillance (CPD). Les droits de procédure sont régis par les articles 36, 37 et 38 LPD.

La personne concernée peut saisir la CPD directement sur requête (art. 36) ou sur recours contre une décision de l'autorité administrative (cf. art. 44 al. 2). Cependant, dans la plupart des cas, les requêtes doivent être adressées à l'autorité administrative qui est maître du fichier. Celle-ce doit rendre une décision, susceptible d'opposition, puis de recours à l'autorité de surveillance.

Il faut signaler le cas particulier des données de police. En cas de requête d'une personne concernée, la police ne rend pas elle-même une décision. Elle communique la requête avec son préavis à la CPD qui tranche.

Communication des données

Des données à caractère personnel peuvent être communiquées à des autorités ou à d'autres organes publics et à des organisations privées, aux conditions posées par les articles 13 et suivants LPD.

Les principales conditions auxquelles la communication des données est subordonnée sont les suivantes :

– la loi réserve d'abord le secret de fonction. Le secret porte sur des faits dont un fonctionnaire a connaissance dans

l'exercice de ses fonctions et qui doivent rester secrets en raison de leur nature, des circonstances ou d'instructions spéciales (cf. art. 25 LStFM). Il frappe donc des faits qui ne sont pas destinés à être connus des tiers. Ce sont avant tout des secrets de nature privée. Le secret de fonction peut être levé lorsqu'aucun intérêt public ou privé prépondérant ne s'y oppose (Knapp, *Précis du droit administratif*, 4e éd., no 58).

Voici les conditions énumérées par la loi pour permettre la communication de données à caractère personnel :

– le responsable du fichier est tenu ou autorisé par la loi à communiquer des données à des autorités ou à d'autres organes publics (art. 13 let. a LPD). Dans cette hypothèse, le secret de fonction n'entre pas en ligne de compte ;

– lorsque le requérant établit qu'il a absolument besoin de ces données pour l'exécution de ses tâches légales (art. 13, let. b LPD), il se justifie, le cas échéant, de lever le secret frappant lesdites données (intérêt public) ;

– de même, lorsque la communication sert les intérêts de la personne concernée et que celle-ci y a expressément consenti (art. 13 let. c LPD). C'est alors le maître du secret (la personne concernée) qui le lève.

Bien entendu, les données qui peuvent être communiquées ne sont pas toutes de nature à rester secrètes. Néanmoins, leur communication doit obéir aux exigences de l'art. 13 LPD.

Communications de données

S'agissant de la communication à des organisations privées, elle est possible aux même conditions que ci-dessus, sauf en ce qui concerne l'exécution d'une tâche légale, – toujours sous réserve du secret de fonction – lorsque le responsable du fichier y est tenu ou autorisé par la loi, ou lorsque la communication sert les intérêts de la personne concernée et que celle-ci y a expressément consenti.

Les conditions posées par la loi à la communication de données sont alternatives et non cumulatives. D'autres dispositions, spéciales, régissent la communication des données à caractère personnel. Les communes sont particulièrement concernées :

– art. 14 al. 3 LPD : la liste des électeurs d'une commune peut être communiquée aux personnes et groupements qui en font la demande.

Cette disposition s'applique aux personnes ou groupements à caractère politique : partis, comités d'initiative ou référendaire, dans le cadre d'élections ou de consultations populaires.

– art. 14 al. 4 LPD : la communication de données à caractère personnel destinée à l'établissement de listes, d'annuaires d'adresses et d'ouvrages similaires est interdite.

L'administration a, par exemple, l'interdiction de publier ou de communiquer la liste des détenteurs de véhicules, mais aussi la liste des jeunes âgés de 16 à 20 ans ou des personnes retraitées ou des membres des associations sportives ou culturelles, sous réserve de l'article 15 al. 3 LPD.

– L'article 15 LPD régit la communication des données par le contrôle des habitants. Cet article concerne donc au premier chef les communes. Nous sommes d'avis que les dispositions contenues à l'article 15 sont applicables par analogie à d'autres autorités administratives qui, dans le cadre des compétences qui leur sont attribuées par la loi, traitent des mêmes données.

– art. 15 al. 1 : ce sont des données courantes qui sont visées ici, accessibles à tout un chacun (nom, adresse, état civil, etc.). Elles sont communiquées si le requérant invoque un intérêt légitime, qui peut être un intérêt de fait ;

– art. 15 al. 3 : cette disposition permet au contrôle des habitants de communiquer à une personne privée des données à caractère personnel selon un classement systématique. Les conditions de cette communication sont strictes :

– les données communiquées doivent servir exclusivement à des fins idéales, c'est-à-dire non commerciales ou lucratives ; ces fins idéales doivent être dignes d'être soutenues, ce qui doit être apprécié de cas en cas ;

– le requérant doit s'engager à ne pas les communiquer à des tiers ;

Pour s'assurer que cette dernière condition soit respectée, l'autorité devra parfois s'abstenir de communiquer une liste de données au requérant et procéder elle-même, le cas échéant, à l'envoi du message. L'autorité doit veiller, en effet, à ce que la communication de données selon un classement systématique n'aboutisse pas à la création, interdite, d'établissement de listes, d'annuaires d'adresses ou d'ouvrages similaires. Une application souple de l'art. 15 al. 3 permettrait, en effet, d'éluder la norme de l'art. 14 al. 4. En tout état de cause, le requérant doit motiver sa requête et établir à quelle fin il utilisera les données qui lui auront été communiquées.

A notre sens, il faut ajouter une autre condition, qui n'est pas prévue expressément par la loi : la communication de données selon un classement systématique ne peut pas porter sur des données sensibles, en particulier lorsqu'elles portent sur des informations relatives à la sphère intime. En revanche, les données qui, par leur nature, sont accessibles à tout un chacun, peuvent faire l'objet d'une communication selon un classement systématique, aux conditions exposées ci-dessus.

Des obligations supplémentaires et problématiques

En conclusion, les communes jurassiennes sont, en matière de protection des données, soumises au même régime que celui qui s'impose aux autorités cantonales. Toutefois, elles doivent, en plus, appliquer des dispositions spéciales (art. 14 et 15 LPD), et ce sont ces dernières qui posent, dans la pratique, le plus de problèmes. Force est de constater que les autorités communales font, encore actuellement, une application très variée de la loi, allant du laxisme le plus large jusqu'à une rigueur des plus tatillonnes. Le rôle de la CPD est d'unifier ces pratiques.

Cette tâche est difficile à exécuter, compte tenu des moyens logistiques peu importants dont dispose l'autorité de surveillance. Bien souvent, elle doit se contenter de sanctionner seulement les abus auxquels conduit la non-observation des dispositions légales. Parfois, elle doit intervenir pour éviter qu'un respect trop strict de la loi provoque une paralysie des activités. Entre ces deux pôles, on est encore loin de l'uniformisation souhaitée. ■