Rapport d'activité du Bureau pour la surveillance de la protection des données

Autor(en): **Siegenthaler**

Objekttyp: **Article**

Zeitschrift: **Verwaltungsbericht des Regierungsrates, der kantonalen Verwaltung und der Gerichtsbehörden für das Jahr ... = Rapport de gestion du Conseil-exécutif, de l'administration cantonale et des autorités judiciaires pendant l'année ...**

Band (Jahr): **- (1997)**

Heft [2]: **Rapport de gestion : rapport**

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-544946

3. Rapport d'activité du Bureau pour la surveillance de la protection des données

3.1 Introduction

3.1.1 1997 en bref

Les services cantonaux ont élaboré les bases nécessaires à l'utilisation d'Internet pour l'échange d'informations, de sorte qu'il a fallu aborder les problèmes de protection des données que soulève ce nouvel auxiliaire. L'introduction d'un système de courrier électronique avec possibilité de cryptage a clairement démontré la nécessité de poser des règles aux niveaux international et national. La formation du personnel cantonal dans le domaine de la sécurité informatique a pu commencer. Enfin, il a été possible *in extremis* d'empêcher provisoirement la transmission de codes de diagnostic très détaillés aux assureurs par les hôpitaux publics.

3.1.2 Collaboration avec le préposé fédéral à la protection des données, quatrième Conférence suisse des délégués à la protection des données

La quatrième Conférence suisse des délégués à la protection des données a été organisée par le canton du Tessin. Elle a adopté une résolution demandant aux assureurs et aux hôpitaux de renoncer à joindre aux décomptes des données très détaillées concernant les diagnostics, et cela juste au moment où les parties s'engageaient à se transmettre de telles données. Le préposé fédéral à la protection des données (PFPD) est compétent dans le cas des assureurs, alors que les hôpitaux relèvent des bureaux cantonaux pour la surveillance de la protection des données. Ce n'est que grâce à la coopération existant entre ces deux niveaux de surveillance qu'il a été possible de stopper provisoirement le processus (cf. ch. 3.9.1).
La question des conditions posées par le droit fédéral à un accès en ligne de l'Intendance des impôts à la banque de données de l'Office de l'agriculture reste ouverte, à l'instar de celle de l'accès du Contrôle des finances à la banque de données des actes de défaut de biens de l'Intendance des impôts.
Enfin, le préposé fédéral a attiré l'attention du Bureau sur le fait que des services cantonaux reliés à plusieurs systèmes informatiques fédéraux relevant de la police n'étaient pas en mesure de satisfaire pleinement aux nouvelles exigences qui seront valables dès le 1er juillet 1998 en matière de sécurité. C'est en effet à cette date que prendra fin le délai transitoire accordé par la loi fédérale sur la protection des données, et à partir de là, les données particulièrement dignes de protection ne pourront plus être transmises que cryptées.

3.2 Description des tâches, priorités, moyens à disposition

3.2.1 Priorités

Le Bureau tente désormais de traiter un maximum de dossiers comme des affaires courantes, c'est-à-dire des affaires à liquider dès leur réception. Cette solution répond aux attentes des clients et diminue, bien que dans une faible mesure, le volume de travail. Il en découle toutefois inévitablement une prolongation des délais d'attente pour les autres affaires, et c'est ainsi qu'une commune a patienté 21 mois pour une étude approfondie portant sur la communication du nom des nouveaux arrivants. Les priorités sont les suivantes: 1) les projets informatiques, 2) la législation générale plutôt que la législation spéciale, 3) les directives générales plutôt que les cas particuliers, 4) les conseils et l'instruction plutôt que les inspections, 5) les problèmes concernant un grand nombre de personnes plutôt que ceux touchant quelques rares individus et risquant peu de se reproduire. Il n'est pas possible de procéder à des inspections compte tenu du nombre sans cesse croissant d'affaires à traiter.

3.2.2 Responsabilité propre des services traitant des données

En 1997 également, de nombreux services se sont renseignés sur l'admissibilité du traitement de certaines données. Outre les cours de perfectionnement usuels, les Directions ont organisé une formation de base dans le domaine de la sécurité informatique (cf. 3.3). Le Bureau a par ailleurs été de plus en plus appelé à prendre position sur des questions de protection des données dans le cadre de procédures administratives ou en droit privé (cf. ch. 3.4, fin). Il est arrivé plus fréquemment que des services informent le Bureau des mesures de protection des données qu'ils avaient prises de leur propre chef (p.ex. lors du tournage d'un film policier à la Direction de l'économie publique). Dans le rapport précédent, le Bureau constatait que tous les cadres ne vouaient pas suffisamment d'attention aux problèmes relevant de la protection et de la sécurité des données. Il était peu probable que cette attitude évolue en l'espace d'une année, et la remarque reste valable. La Direction de la justice, des affaires communales et des affaires ecclésiastiques a toutefois donné un important signal en adoptant avec la Cour suprême un cahier des charges commun sur le comité de contrôle de la sécurité informatique, comité présidé par le secrétaire général. Il est également réjouissant de constater que la Direction de l'instruction publique a soumis un projet de directives relatives aux PC qui décrivent notamment la fonction du délégué à la protection des données interne à la Direction.

3.2.3 Rapport entre moyens informatiques et moyens mis à la disposition de la protection et de la sécurité des données

Selon les renseignements fournis par l'Office d'organisation, les investissements prévus dans le domaine informatique se montaient à 21,5 millions de francs en 1997, alors que 120,6 millions de francs devaient être consacrés à l'exploitation des auxiliaires de TED (montants budgétés). Quant au coût total du Bureau, il s'est maintenu à quelque 0,25 million de francs. Le responsable de la sécurité informatique de la Direction de la justice, des affaires communales et des affaires ecclésiastiques a procédé à quelques contrôles simples dans les administrations de district. Il a par exemple examiné les mots de passe utilisés, ce qui a déjà en soi impliqué une somme de travail considérable. Il est hors de question de procéder aux examens à la fois permis et rendus nécessaires par l'informatique, comme l'évaluation des données journalisées dans des procès-verbaux. La constatation selon laquelle les

ressources affectées aux mesures et aux contrôles en matière de protection et de sécurité des données sont insuffisantes par rapport aux dépenses consenties dans le domaine de l'informatique se confirme une fois de plus.

3.2.4 Nouvelles tâches

Le Conseil-exécutif a réglementé d'une part l'exploitation du réseau grande distance du canton de Berne BEWAN, et d'autre part la mise en service et l'utilisation d'Internet. Les deux arrêtés confient de nouvelles tâches au Bureau (suivi de BEWAN, suivi des activités sur Internet et participation à la Commission Web). Dans ses prises de position au sujet des deux arrêtés, le Bureau a clairement indiqué qu'il ne serait en mesure d'accomplir ses nouvelles tâches que s'il était doté de ressources supplémentaires. Or, de telles ressources n'ont pas été mises à sa disposition. Ce cas est d'ailleurs exemplaire: les tâches qui incombent au Bureau de par la loi augmentent, alors que les moyens dont il dispose restent les mêmes. En conséquence, le Bureau est de moins en moins en mesure de s'acquitter de son mandat légal.

3.2.5 Registre

Faute de ressources, le registre ne contient guère de données supplémentaires par rapport aux années précédentes. Il en résulte que le mandat légal de base (saisie de tous les fichiers) n'est toujours pas rempli, et que les informations relatives aux 812 fichiers enregistrés n'ont été ni contrôlées sous l'angle juridique, ni mises à jour. Le chiffre 3.7 renseigne sur les registres des collectivités de droit communal.

3.3 Sécurité des données

La classification des applications informatiques exigée par l'arrêté du Conseil-exécutif 4637/92 (avec un délai initialement fixé à fin 1994) n'existe toujours pas à la Direction des travaux publics, des transports et de l'énergie (qui n'a produit qu'une estimation) et n'a pas été établie dans la forme prescrite par la Direction de la justice, des affaires communales et des affaires ecclésiastiques (qui dispose toutefois d'un rapport sur la sécurité allant plus loin que ne le demande l'ACE). Par manque de temps, l'exactitude des classifications fournies par les autres Directions n'a toujours pas fait l'objet d'un examen (cf. toutefois ch. 3.4), et il en va de même de la mise en œuvre des mesures prévues.
Deux Directions se sont dotées, au niveau interne, d'organes chargés du contrôle de la sécurité (cf. ch. 3.2.2) en réponse notamment à l'intervention Galli. La sécurité informatique implique des consignes précises. A cet égard, la directive S02 de l'Office fédéral d'informatique et les documents y afférents (manuel) permettent de concrétiser utilement, au niveau cantonal aussi, l'obligation énoncée dans la loi sur la protection des données de prendre des mesures pour garantir la sécurité des données.
Dans sa réponse à l'interpellation Koch, le Conseil-exécutif a précisé les mesures prises dans la perspective du changement de millénaire, mesures dont le coût sera probablement supérieur à cinq millions de francs.
Toute personne employée par le canton de Berne qui travaille sur un ordinateur doit connaître les risques existant en matière de sécurité des données et être en mesure d'y faire face. La formation dans ce domaine, étendue à tout le personnel, a commencé en 1997. Elle se fonde sur le CD didactique et interactif «SAVE». Ce CD a été élaboré sous la responsabilité de l'Office d'organisation par une équipe d'experts de la sécurité et de spécialistes de l'administration cantonale, avec la participation de la cheffe du Bureau de l'égalité entre la femme et l'homme et du délégué à la protection des données. Le consortium privé chargé de l'élaboration du CD, qui a participé à son financement, l'utilise – sans les informations spécifiquement bernoises – comme base en vue d'un CD destiné à la formation générale en matière de sécurité informatique.

3.4 Projets informatiques

Le projet GEFnet de la Direction de la santé publique et de la prévoyance sociale vise la création d'un réseau interne à la Direction et le remplacement de l'ordinateur central existant. Or, des données particulièrement dignes de protection sont traitées, en particulier à l'Office du médecin cantonal, dans le domaine de l'asile ainsi que dans le cadre des conseils aux victimes d'infractions. Il s'est donc agi de formuler dans le cahier des charges des exigences suffisamment strictes en matière de protection et de sécurité des données. Il existe en effet un risque que la sécurité soit compromise par des interférences entre le réseau interne et le réseau grande distance BEWAN, de sorte que les offres devront proposer des solutions à ce problème.
Le projet ZBD du Service de l'état civil et de l'indigénat de la Direction de la police et des affaires militaires doit remplacer par un réseau propre au service le traitement de texte et le contrôle des affaires utilisés jusqu'ici. Du fait que cette (petite) entité administrative est située bien à l'écart, il est possible de renoncer, malgré le caractère très confidentiel de certaines des données traitées, à un cryptage généralisé des données échangées au plan interne. S'agissant des documents sensibles, il sera possible, le cas échéant, de recourir aux modalités de cryptage du courrier électronique proposées par le système BEMAIL. La stratégie informatique de la Direction de la police et des affaires militaires contient un classement incorrect des degrés de confidentialité des données et doit par conséquent être corrigée.
Dans le cas du système KOMKonzept II de l'administration de l'université (transfert, par le réseau de l'université, de données cryptées concernant des décomptes médicaux), le Bureau a constaté qu'une clé de faible longueur pouvait être utilisée dans un premier temps à condition qu'une extension soit possible.
Dans une prise de position relative à un projet partiel découlant du projet «Bourses 97» de la Direction de l'instruction publique, il s'est agi de déterminer à quelles conditions les demandes de bourses pourraient être formulées par le biais d'Internet. Le projet débordait toutefois le champ d'application de la loi bernoise sur la protection des données (questions procédurales, communication de données par des particuliers).

3.5 Législation

Le Grand Conseil a adopté plusieurs modifications législatives visant à délier l'école ainsi que les autorités d'assistance et de tutelle de l'obligation d'informer prévue par le Code de procédure pénale lorsque la commission d'un crime est soupçonnée. La loi sur la police a été adoptée lors d'un scrutin populaire. Le parlement a décidé d'autoriser l'Institut de médecine légale à accéder par une procédure d'appel aux données de la police cantonale dont il a besoin. Certains voient dans cette réglementation la base légale de la création d'une banque de données du patrimoine génétique (fichier des traces ADN) au service des autorités de poursuite pénale. Le Bureau ne partage toutefois pas cette opinion: l'importance considérable que revêt une telle banque de données pour ces autorités exclut que la base légale en soit créée subrepticement.

L'ordonnance sur l'organisation et les tâches de la Direction de la justice, des affaires communales et des affaires ecclésiastiques a été modifiée en ce sens que les responsables de l'informatique sont subordonnés à la Cour suprême lorsqu'ils travaillent sur les systèmes informatiques des tribunaux.

3.6 Internet, sécurité du courrier électronique

3.6.1 Internet

Le Conseil-exécutif a adopté le 2 juillet des directives concernant la mise en service et l'utilisation d'Internet et des offres présentées sur le Web par l'administration cantonale. Il a ainsi précisé les modalités selon lesquelles le canton peut fournir des informations par le biais d'Internet et d'Intranet. Il appartient par ailleurs aux Directions de définir les personnes qui, au sein de l'administration, doivent avoir accès à Internet. Le Bureau a d'emblée participé à l'élaboration des directives en question. Il a notamment attiré l'attention sur le rapport édité en mai 1996 par l'Office fédéral de la justice, rapport établi par un groupe de travail interdépartemental sur les questions de droit pénal, de protection des données et de droit d'auteur soulevées par l'utilisation d'Internet. Une contribution du préposé fédéral à la protection des données figure dans ce rapport. Le recours à Internet peut porter atteinte à la protection de la personnalité dans les cas suivants: a) personnes dont le canton communique des données par Internet (cf. ch. 3.1.3 du rapport de 1996), b) personnes qui consultent les offres du canton, c) membres du personnel qui accèdent aux informations fournies par Internet (cf. ch. 3.7.4 du rapport de 1996). Le canton ne dispose d'aucune base légale pour traiter des données concernant les visiteurs de ses pages Internet. La question de la sécurité se pose en ces termes: il s'agit de minimiser les risques qu'Internet fait courir au réseau cantonal et aux applications qui y sont reliées. Or, la surveillance de l'interface avec Internet (ordinateur coupe-feu) est une tâche très complexe puisqu'il convient de réagir immédiatement à toute nouvelle menace connue. Il n'existe toutefois pas d'accès à Internet qui soit absolument sûr. Par ailleurs, les pages Internet du canton peuvent également être prises pour cibles (modification du contenu, création de liens hypertexte). Il est indispensable, enfin, d'empêcher que des informations confidentielles soient par erreur stockées à un endroit accessible par le biais d'Internet. Le Bureau soutient la démarche active du Conseil-exécutif, sans pour autant ignorer les risques qui y sont liés. Faute d'une solution valable pour l'ensemble de l'administration en effet, des solutions individuelles seront développées pour l'utilisation d'Internet, avec des risques accrus à la clé. Un recours à Internet qui satisfasse aux exigences de la protection des données requiert d'une part le développement constant de nouvelles mesures visant à garantir la sécurité des données, et d'autre part la prise en considération des nouvelles atteintes portées à la personnalité. Pour respecter la législation, l'utilisation d'Internet devra impérativement entraîner à tous les niveaux l'octroi de ressources supplémentaires pour le suivi des questions de protection des données.

3.6.2 Sécurité du courrier électronique

Avec le projet BEMAIL, le canton entend introduire également le transfert de messages cryptés. L'interdiction de transmettre des données particulièrement sensibles (ACE 3457/95) ne pourra être levée qu'à condition qu'un système de cryptage soit disponible. De tels systèmes existent et sont techniquement satisfaisants (systèmes à clé publique). Quant à la certification des clés, elle est également réalisable. Si la technique est très avancée dans ce domaine, il n'en va pas de même des réglementations: c'est ainsi que différentes questions restent en suspens, dont celles de savoir comment l'autorité de certification transmet les clés aux ayants droit, comment elle doit vérifier l'identité de ces derniers, quelle est sa responsabilité, quelles sont les conditions techniques d'une conservation des clés par l'ayant droit, et quelle doit être la durée de validité d'un certificat. La législation allemande sur la signature fournit des indications importantes à cet égard. Le niveau de sécurité atteint à ce jour par le canton de Berne n'est pas entièrement conforme aux exigences allemandes (utilisation de cartes à puce). Si la solution bernoise semble suffisante en ce qui concerne le transfert de données sensibles (confidentialité), il n'est pas encore possible de franchir le pas de la signature électronique (validité). Il est frappant de constater, à cet égard, que seules des normes coordonnées aux niveaux international et national permettent un échange de documents offrant toutes les garanties du point de vue de la confidentialité et de la validité. Le fait qu'un système de courrier électronique interne à l'administration dépende de tels standards souligne bien l'urgence du problème.

3.7 Collectivités de droit communal

Le Bureau a publié dans le recueil «Information systématique des communes bernoises» (ISCB) des avis concernant la communication de données aux paroisses par le contrôle des habitants et l'examen du bien-fondé des déductions fiscales.
La commune de Wohlen a achevé son registre des fichiers.
Deux syndicats hospitaliers ont renoncé, suite à l'intervention du Bureau, à adresser à leurs patients sans y avoir été invités des décomptes téléphoniques mentionnant tous les numéros appelés.
Enfin, le Bureau a attiré l'attention de l'Association des secrétaires communaux sur les problèmes informatiques engendrés par le changement de millénaire, problèmes qui concernent également les collectivités de droit communal.

3.8 Points abordés dans le rapport précédent

3.8.1 Centrale des amendes d'ordre

Le système informatique choisi par la centrale des amendes d'ordre conduit, pour des motifs comptables, à un enregistrement illicite des débiteurs d'amendes. Le Commandement de la police avait assuré en 1995 déjà qu'il serait remédié à cette situation. Dans son rapport de 1996, le Bureau a déploré le fait qu'aucune mesure n'avait encore été prise. La Direction de la police et des affaires militaires a ensuite fait savoir, dans une directive datée du 30 décembre 1997, qu'elle renonçait pour des raisons financières à l'adaptation requise du programme (mesure technique), et qu'un remplacement devait être prévu pour l'an 2000 ou 2001. D'ici là, le système informatique doit être utilisé aux fins prévues par la législation sur les amendes d'ordre uniquement, et toute tentative d'exploitation à d'autres fins doit être communiquée sans délai au Commandement de police. Enfin, il y a lieu d'informer chaque semestre le secrétariat général de la mise en œuvre de la directive (mesure organisationnelle). Avec un tel document, la Direction de la police et des affaires militaires assume la responsabilité de son choix de conserver le programme inchangé, ce qui représente un pas décisif vers une répartition claire des responsabilités. Il importe encore que les mesures organisationnelles fassent leurs preuves dans la pratique. En tout état de cause, la Direction de la police et des affaires militaires fait passer les intérêts financiers avant ceux de la protection des données, et le Bureau estime la pesée des intérêts incorrecte en l'espèce. Contrairement aux particuliers, il n'a toutefois plus aucune possibilité d'intervention.

3.8.2 Projet informatique KOBI de la Police cantonale

Au chiffre 3.4 de son rapport de 1996, le Bureau relevait qu'avec son projet informatique KOBI, le Commandement de la police avait testé le recours à un ordinateur (portable ou non) permettant aux collaborateurs de la police d'interroger en une seule opération, c'est-à-dire sans répéter la procédure d'identification, les données concernant une personne précise contenues dans plusieurs banques de données. Le Bureau avait attiré l'attention sur la violation des règles imposant le traitement séparé des données de certaines banques rendue possible par le système KOBI. En effet, la combinaison automatique de possibilités d'interrogation reposant individuellement sur une base légale suffisante représente pour les personnes concernées une atteinte nettement accrue à leur droit fondamental à la protection des données, et cette atteinte requiert à son tour une base légale. Un tel système pose en outre des problèmes de sécurité du fait qu'il repose sur un seul mot de passe universel. Enfin, le principe de la proportionnalité doit être observé même en présence d'une base légale. Dans une lettre du 24 décembre, la Direction de la police et des affaires militaires a indiqué qu'elle avait autorisé l'utilisation du système KOBI d'entente avec le procureur général, et que cette décision avait notamment été rendue nécessaire pour des raisons techniques de transmission. La lettre ajoutait que ce système sert avant tout à garantir l'efficacité du travail accompli par la police judiciaire et la police de sûreté, et que cet aspect prime celui de la protection des données. Là encore, le Bureau ne partage pas l'avis de la Direction de la police et des affaires militaires. Il estime toutefois positif que cette dernière ait fourni des informations précises sur sa décision et qu'elle assume la responsabilité de l'utilisation du système KOBI. Les questions de droit pourraient le cas échéant être traitées suite au recours d'une personne concernée, ou lorsque le Conseil-exécutif sera appelé à autoriser les systèmes informatiques de la police (nouvelle loi sur la police).

3.9 Cas particuliers

3.9.1 Communication de données par les hôpitaux aux assureurs

La Fédération cantonale bernoise des assureurs-maladie et l'Association des établissements hospitaliers bernois ont conclu en date du 10 septembre une convention tarifaire devant entrer en vigueur le 1er janvier 1998. Les hôpitaux se sont notamment engagés à mentionner les codes de recherche CIM-10 et CIM-9 CM sur les décomptes destinés aux assureurs. Or, ces données sont à la fois trop détaillées pour l'examen de l'économicité du traitement et partiellement impropres du fait qu'elles ne contiennent aucune précision sur l'environnement social du patient, pourtant déterminant dans le choix du traitement. Cette convention a un effet contraignant pour les hôpitaux qui l'acceptent; or, presque tous les syndicats hospitaliers ont donné leur accord, certains en émettant des réserves concernant la protection des données. Par courrier du 5 décembre, le Bureau a recommandé à tous les syndicats de renoncer jusqu'à nouvel avis à la communication des codes de diagnostic en attirant leur attention sur les conséquences en matière de responsabilité ainsi que sur le risque éventuel d'une condamnation pénale. Suite à cette intervention, les deux associations sont convenues de renoncer provisoirement à cet aspect de la convention. Il y a lieu de s'attendre à ce qu'une solution soit trouvée au niveau fédéral entre le préposé à la protection des données et les assureurs (cf. ch. 3.1.2).

Le 21 janvier 1998

Le délégué à la protection des données: *Siegenthaler*