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): **- (1995)**

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

PDF erstellt am: **25.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-418267

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

3.1 Introduction

3.1.1 1995 en bref

En 1995, les services appelés à traiter des données ont dû appliquer pour la première fois la nouvelle législation sur l'information. Ils ont fait preuve de circonspection à cet égard, de sorte que la phase d'introduction n'a pas suscité de problèmes particulièrement épineux. Par ailleurs, l'interconnexion croissante qui caractérise le traitement informatique des données compromet la sécurité de ces dernières. Cette remarque vaut également dans le canton de Berne, comme l'ont notamment confirmé les rapports des services chargés de traiter des données.

3.1.2 Collaboration avec le Préposé fédéral à la protection des données

La deuxième conférence suisse des délégués à la protection des données a eu lieu le 20 octobre 1995. Dans une résolution commune, les participants ont demandé qu'un droit de blocage inconditionnel permette de s'opposer à l'obtention de données concernant les détenteurs de véhicules par le biais du numéro de téléphone 111 et du vidéotex; ils ont également suggéré le réexamen de la nécessité de publier de telles données. Dans le canton de Berne, il existe toutefois un droit de blocage inconditionnel dans le domaine en question.
L'importance des recommandations formulées par le Préposé fédéral (ou devant encore l'être) en matière de sécurité des données informatisées a été relevée lors de la conférence. Le rapport d'activité 1994 du Bureau bernois pour la surveillance de la protection des données évoquait les problèmes engendrés par la liste des analyses du Département fédéral de l'intérieur (diagnostic du sida figurant sur des décomptes destinés aux caisses-maladie). Or, il ressort du 2e rapport d'activité du Préposé fédéral que la nouvelle liste entrée en vigueur le 15 mars 1995 apporte un début de solution à ce problème.

3.1.3 Droit international

Le 13 décembre, le Conseil-exécutif a édicté dans son arrêté 3457/95 des «directives concernant l'utilisation du système de messagerie électronique BEMAIL, la télémaintenance et les raccordements à Internet». Cet arrêté admet que l'un des nœuds du réseau cantonal de messagerie électronique restera provisoirement à Warwick, en Angleterre (cf. restrictions faites par le Conseil-exécutif sous ch. 3.4). Les recommandations figurant dans le 15e rapport d'activité du Commissaire fédéral allemand chargé de la protection des données au sujet de l'exploitation de systèmes de courrier électronique constituent l'une des bases essentielles de l'arrêté. Les échanges de données à l'échelle internationale sont notamment très fréquents dans le cadre de projets de recherche menés par l'Université. Dans le domaine particulièrement délicat de la recherche médicale, il y a lieu d'espérer que les conditions d'ordre général posées par le droit fédéral contribueront à résoudre le problème à long terme. Le recours accru aux technologies médicales de pointe entraîne un besoin croissant de télémaintenance. A cet égard, la télémaintenance d'appareils médicaux se trouvant dans le canton de Berne (qui implique l'accès aux données concernant les patients) a également lieu à partir de l'étranger.

3.2 Description des tâches, priorités, moyens à disposition

3.2.1 Priorités

Dans sa réponse à l'interpellation Galli (optimisation de la protection des données), le Conseil-exécutif a confirmé l'impossibilité d'accroître les ressources destinées à la surveillance de la protection des données, ce qui a immanquablement pour conséquence «que la surveillance de la protection des données prescrite tant par la loi cantonale sur la protection des données que – dans le cadre de la mise en œuvre du droit fédéral – par la loi fédérale du même nom ne peut avoir lieu que dans des proportions restreintes». Dans ce contexte, il n'est pas inutile de répéter que la pénurie de ressources a impliqué de fixer des priorités avec un soin tout particulier, en tenant compte des critères suivants: 1) la législation générale plutôt que la législation spéciale, 2) le suivi de projets informatiques lors de la phase de planification, 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. L'importance de l'information en tant qu'instrument de travail reste considérable, et cela dans tous les domaines. Le suivi de projets informatiques constitue quant à lui un élément nouveau. Le dernier rapport d'activité relevait la nécessité d'un contrôle des grands systèmes informatiques, et cette remarque conserve toute sa validité. En effet, même des applications informatiques correctement planifiées peuvent susciter des problèmes, comme en témoigne l'utilisation du système KOFINA (Administration des finances) par la centrale des amendes d'ordre: afin d'éviter l'attribution de plusieurs numéros de débiteurs, le système enregistre les amendes d'ordre infligées au cours des trois dernières années en fonction des numéros de plaques minéralogiques. Cette solution choisie pour des motifs comptables aboutit à un enregistrement susceptible d'être utilisé à des fins policières. Rien ne permet toutefois d'affirmer qu'un tel usage a été fait des données ainsi disponibles et d'ailleurs, les services de la police cantonale concernés se sont déclarés disposés à faire modifier le système. Ce qu'il convient de retenir de cet exemple, c'est que l'erreur a été décelée grâce aux indications fournies par une personne concernée, et pas dans le cadre d'un contrôle ordinaire (puisqu'il n'y en a justement pas). Il ressort des examens proposés par certaines sociétés fiduciaires et portant avant tout sur la sécurité des données qu'un contrôle systématique des grands systèmes informatiques sous l'angle de la protection des données occasionne une dépense pouvant rapidement atteindre quelque 100 000 francs. Or, le Bureau ne dispose pas de crédits, de sorte que seule la mobilisation de ressources humaines pourrait entrer en ligne de compte s'il n'y avait insuffisance des effectifs d'une part, et manque d'informaticiens d'autre part. Faute de solution, les contrôles des grands systèmes informatiques que le Bureau est en mesure d'effectuer (généralement parce que des circonstances extérieures l'y ont incité) doivent être qualifiés de trop superficiels.

3.2.2 Responsabilité propre des services

Dans sa réponse à l'interpellation Galli, le Conseil-exécutif a encore relevé que les services cantonaux sont en fin de compte eux-mêmes responsables du respect des prescriptions contenues dans la législation sur la protection des données et qu'il leur appartient, compte tenu des moyens dont ils disposent, de fournir les ressources tant humaines que matérielles nécessaires à tous les niveaux pour veiller au respect de ces prescriptions. Une institution en particulier les a respectées de manière exemplaire: l'hôpital de l'Ile, qui s'est doté de son propre délégué à la protection des données à fonction accessoire depuis le 1er juillet. Il convient également de mentionner les cours internes de perfectionnement organisés par les offices cantonaux d'orientation en matière d'éducation en collaboration avec le Service pédo-psychiatrique, de même que par les établissements de Witzwil. La Cour suprême a pour sa part établi le registre des fichiers concernant son domaine au cours de 1995. Dans le Manuel de l'aide sociale qu'elle est en train d'élaborer, la Direction de la santé publique et de la prévoyance sociale (Office de prévoyance sociale) expose notamment, sous un angle pratique, les problèmes touchant à la protection des données à l'intention des services exécutants. Les écoles de l'hôpital de l'Ile ont quant à elles réglé la question de la conservation des dossiers dans des directives détaillées. Certains points négatifs doivent toutefois aussi être signalés, dont un problème de taille: les organes dirigeants n'ont pas suffisamment pris conscience de l'importance de la sécurité des données dans le domaine informatique (cf. ch. 3.4). Il est révélateur, à cet égard, que la procédure de corapport concernant l'arrêté du Conseil-exécutif 3457/95 (BEMAIL) ait été pour l'essentiel confiée aux responsables de l'informatique. Le fait qu'un service informatique ait dû avoir recours à une prise de position du Bureau pour convaincre un chef d'office de ne pas installer un ordinateur central dans une cafétéria accessible au public est quelque peu inquiétant. A cet égard, le document relatif à la sécurité des données que la Direction de la justice, des affaires communales et des affaires ecclésiastiques a fait élaborer par des entreprises externes contient la phrase suivante: «La prise de conscience du caractère indispensable des mesures de sécurité et de contrôle dans le domaine informatique est insuffisante, notamment chez les responsables de la gestion» (traduction). Cette affirmation pourrait se révéler encore plus vraie dans d'autres services.

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

L'Office d'organisation indique qu'en 1995, les investissements se sont montés à 20 millions de francs dans le domaine informatique, et que 118 millions ont été consacrés à l'exploitation des auxiliaires de TED. Quant au coût total du Bureau, il s'est maintenu autour de 0,25 million de francs. Comme il a déjà été dit dans le rapport précédent, il serait judicieux de fixer les dépenses consacrées au Bureau en fonction des ressources mises à la disposition de l'informatique. Or, les problèmes existants n'ont rien perdu de leur acuité en 1995. Le rapport demandé par la Direction de la justice, des affaires communales et des affaires ecclésiastiques montre que la sécurité (indépendamment des tâches du Bureau) ne saurait être garantie sans une importante mobilisation de ressources. L'étude s'est fondée sur 1200 postes de travail standards équipés des dispositifs de sécurité habituellement disponibles sur le marché. Ainsi, les mesures organisationnelles de sécurité ordinaires étaient déjà prises. A partir d'un ordre de priorités détaillé, le rapport indique que la garantie d'un niveau de sécurité approprié entraîne les frais supplémentaires suivants: 500 000 francs de dépenses uniques, 662 jours de travail dans la phase initiale, puis 220 jours chaque année. Le rapport lui-même a été facturé à 80 000 francs. Ces chiffres témoignent bien du coût de la sécurité des données traitées par le biais de l'informatique. Ils révèlent encore mieux à quel point les mandats de contrôle que la loi sur la protection des données (art. 34, lit. b et e) confie au Bureau peuvent facilement rester lettre morte.

3.2.4 Nouvelles tâches

Le nouveau Code de procédure pénale entrera en vigueur le 1er janvier 1997. Contrairement à l'ancien Code, il place les enquêtes de police sous la surveillance du Bureau (cf. ch. 3.6.2). Or, la mise en œuvre de cette prescription implique de nouvelles ressources, et si ces dernières ne sont pas mises à disposition, le Bureau se trouvera d'une part dans l'impossibilité d'accomplir ses nouvelles tâches, en tout cas intégralement, et d'autre part dans l'obligation de réduire ses autres activités.

3.3 Registre

Fin 1995, 809 fichiers avaient été introduits dans le programme «Sisyphus». Ce dernier a été provisoirement installé à la Cour suprême et à la clinique psychiatrique de Münsingen en 1995, en vue de la saisie des données.

3.4 Sécurité des données

Cinq Directions sur sept ont présenté fin 1995 la classification de leurs applications informatiques exigée par l'arrêté du Conseil-exécutif 4637 du 9 décembre 1992 (le délai avait été initialement fixé à fin 1994). La Direction des travaux publics, des transports et de l'énergie a produit une estimation provisoire en lieu et place du classement demandé. La Direction de la justice, des affaires communales et des affaires ecclésiastiques a quant à elle présenté un rapport sur la sécurité élaboré par des organes externes. Du point de vue matériel, ce rapport va plus loin que ne le demandait l'ACE 4637/92, même si la classification des applications informatiques à proprement parler doit encore avoir lieu à un stade ultérieur et n'était par conséquent pas disponible fin 1995. Il y a désormais lieu d'examiner si les classifications établies sont correctes et si les mesures prescrites par l'ACE 4637/92 ont effectivement été prises. Dans sa réponse à l'interpellation Galli, le Conseil-exécutif a chargé la Conférence informatique d'examiner l'opportunité d'instituer un comité de sécurité ou de désigner le responsable informatique de chaque Direction à la fonction de responsable de la sécurité des données d'une autre Direction. Ce faisant, le Conseil-exécutif a souligné l'importance qu'il attache à la garantie d'une sécurité suffisante dans le domaine informatique. La question de savoir si la démarche proposée, qui n'occasionne pas de dépenses supplémentaires, est susceptible d'apporter une solution au problème reste ouverte. La phrase du rapport sur la sécurité de la Direction de la justice, des affaires communales et des affaires ecclésiastiques indiquant que «de l'avis des auteurs du concept, le niveau de sécurité constaté à la JCE est insuffisant, de sorte qu'une intervention s'impose» (traduction) s'est vu accorder l'importance qu'elle méritait puisque la Direction a immédiatement pris des mesures. De plus, le rapport a été demandé avant la réalisation du projet global de mise en réseau (qui englobe toutes les administrations de district et les tribunaux), ce qui permet d'affirmer que la Direction a agi à temps. Ce document a toutefois mis en évidence les problèmes considérables que fait naître le développement fulgurant de l'informatique au niveau de la sécurité. Il n'est pas possible, dans le cadre du présent rapport, de s'étendre davantage sur son contenu qui aborde en particulier les aspects suivants: mot de passe protégeant la mise en veille, désactivation des lecteurs de disquettes des différents postes de travail (notam-

ment à titre de protection contre les virus), amélioration de la documentation relative à la sécurité, acquisition d'extincteurs portatifs à CO_2 pour les locaux abritant les serveurs, «séparation des pouvoirs» entre les administrateurs des systèmes et contrôles dont ces derniers font l'objet afin de respecter les impératifs de sécurité. L'exemple des administrateurs montre bien à quelle vitesse la situation évolue: s'ils ont aujourd'hui accès pour l'essentiel aux données de la Direction de la justice, des affaires communales et des affaires ecclésiastiques à Berne et à celles de deux administrations de district et de deux tribunaux, ils pourront à l'avenir accéder à l'ensemble des données de chaque service administratif décentralisé et de chaque tribunal. Le rapport qu'a fait établir la Direction contient des principes valables pour l'ensemble de l'administration cantonale, raison pour laquelle l'Office d'organisation l'a présenté à la Conférence informatique à l'occasion d'une séance spéciale, mettant ainsi à l'ordre du jour la question de la sécurité dans le domaine informatique. Une version du rapport limitée aux considérations de portée générale pourra d'ailleurs être consultée par les responsables de l'informatique. Il est indéniable que les problèmes liés à la sécurité prennent un relief particulier lors de toute mise en réseau. Une étude préalable commandée dans le cadre du projet BEWAN (réseau étendu du canton de Berne) traite de ces problèmes dans le but d'élaborer un programme concernant la sécurité. A l'instar d'une étude zurichoise plus détaillée sur la sécurité des réseaux (Fakten 1/96), l'étude précitée aboutit à la conclusion que la garantie de la sécurité des données traitées en réseau mobilise des ressources considérables. Cette conclusion confirme le bien-fondé de l'ACE 3457/95 (cf. ch. 3.1.3) et l'on ne peut qu'approuver l'interdiction faite par le Conseil-exécutif de transmettre (entre autres) des données personnelles particulièrement dignes de protection par courrier électronique. Dans son rapport relatif à l'arrêté, le Conseil-exécutif cite une grande multinationale de l'informatique participant au projet selon laquelle «il convient d'admettre qu'aucune communication empruntant un quelconque réseau n'est sûre. La seule protection efficace est le cryptage» (traduction). Le fait d'admettre que la transmission électronique de données non cryptées à l'intérieur d'un réseau n'est a priori pas sûre suscite immanquablement d'autres questions. On peut être amené à examiner l'opportunité d'une intervention dans d'autres domaines caractérisés par la communication de données au moyen d'un réseau informatique. Le premier exemple qui vient à l'esprit est celui des décomptes effectués de manière centrale dans le domaine médical, qui nécessitent le transfert électronique de données non cryptées (dont on peut sans peine admettre qu'elles sont toutes particulièrement dignes de protection). En tout état de cause, le développement fulgurant de l'informatique semble devoir forcément engendrer certaines incohérences. Enfin, le champ d'application de l'ACE 3457 est révélateur, puisqu'il s'étend à tous les organes (y compris externes) qui sont chargés d'effectuer des tâches publiques cantonales et qui sont reliés au système BEMAIL par leurs systèmes de courrier locaux. Il est certes parfaitement correct d'étendre ainsi le champ d'application de l'arrêté, mais ce choix montre bien à quel point l'interconnexion ignore les délimitations traditionnelles des responsabilités. Il convient de relever à cet égard que les établissements autonomes et les tribunaux utilisent le système de messagerie électronique.

3.5 Projets informatiques

Le problème posé par un projet de raccordement on-line de l'Intendance des impôts à la banque de données GELAN de l'Office de l'agriculture a pu être résolu avec les services concernés, qui en ont admis le caractère disproportionné. L'objectif visé était de permettre des contrôles au hasard des déclarations d'impôt remplies par les agriculteurs par le biais d'un accès limité aux décisions concernant le versement de subventions. Toutefois, un tel accès aurait entraîné un flux excessif de données vers l'Intendance des impôts, et cela même si la base légale nécessaire – tout au moins une ordonnance – avait été créée à cet effet, alors qu'un contrôle au moyen de méthodes conventionnelles (envoi des documents sur demande) suffit. Le projet ALIDAT du laboratoire cantonal a soulevé quant à lui des questions ayant trait à la sécurité du réseau. Enfin, les responsables du projet EVOK (mise en œuvre informatisée de la loi fédérale sur l'assurance-maladie) ont demandé un préavis détaillé au Bureau. Il s'est agi non seulement d'étudier les questions relatives à la sécurité des données, mais aussi de déterminer exactement les données dont les principaux intervenants (Office des assurances sociales et de la surveillance des fondations, Intendance des impôts, Caisse de compensation et, indirectement, caisses-maladie et communes) ont besoin pour s'acquitter de leurs tâches respectives. Il a en particulier fallu opérer une distinction entre les données requises pour le contrôle du respect de l'obligation de s'assurer d'une part, et le versement de contributions d'autre part. La solution d'une «ordonnance urgente» limitée dans le temps (ordonnance législative de substitution au sens du droit constitutionnel bernois) en tant que base légale «formelle» à la procédure d'appel a par ailleurs été considérée comme suffisante.

3.6 Législation

3.6.1 Répercussions de la loi fédérale sur la protection des données

Contrairement à la loi fédérale, la loi bernoise sur la protection des données soumet le blocage des données à la preuve d'un intérêt digne de protection, abstraction faite de quelques exceptions. Au niveau fédéral en revanche, il suffit de rendre un tel intérêt vraisemblable. A cet égard, un alignement sur le droit fédéral semble d'autant plus de mise que la législation bernoise sur l'information autorise de manière bien plus large que le droit fédéral la communication à des particuliers de données personnelles qui ne sont pas particulièrement dignes de protection.

3.6.2 Autres actes législatifs cantonaux

La nouvelle réglementation de la protection des données dans le Code de procédure pénale révisé qui entrera en vigueur le 1er janvier 1997 apporte un changement positif. Le fait que les enquêtes de police soient en principe soumises à la loi sur la protection des données (les exceptions concernent avant tout la réunion des données) répond aux exigences du droit fédéral. Les prescriptions applicables à la conservation des données par la police judiciaire tiennent compte de la jurisprudence du Tribunal fédéral. Par contre, l'obligation générale d'informer désormais faite aux agents du canton et des communes en cas d'infraction poursuivie d'office devrait sans doute être nuancée par des prescriptions contenues dans des lois et limitées à certains domaines spécifiques. Des répercussions négatives sont en effet à craindre dans le domaine de l'administration chargée de l'encadrement et de l'assistance (orientation en matière d'éducation, école et jardin d'enfants, prévoyance sociale). C'est ainsi que les personnes apportant leur aide à une victime (p. ex. un enfant maltraité) hésiteront désormais à requérir l'aide des autorités. En tout état de cause, il est frappant de constater que le Bureau s'est vu soumettre des problèmes à la fois complexes et délicats touchant justement à cet aspect de la protection des données. La loi sur la police actuellement en procédure de consultation traite la question de la protection des données en coordination avec le Code de procédure pénale. Elle crée une base légale à la procédure d'appel prévue pour la police et règle les rapports de police relatifs à des personnes (certificats de bonnes mœurs).

3.7 Collectivités de droit communal

En 1995, douze nouveaux règlements sur la protection des données ont pu être approuvés, de sorte qu'à la fin de l'année, 198 communes disposaient de leur propre règlement. Un nouveau règlement type sur la protection des données a dû être établi afin de tenir compte de la législation sur l'information. Il a pu être adressé aux communes par le biais du recueil intitulé «Information systématique des communes bernoises» qu'édite depuis peu l'Office des affaires communales et de l'organisation du territoire, en même temps que d'autres documents (commentaire, modification du règlement type d'organisation, formulaire de demande de blocage des données, liste des textes législatifs). Au début de l'année, les commissions communales de surveillance pour la protection des données ont été rendues attentives à la diminution de la protection des données induite par la législation sur l'information. Elles ont été priées, à cette occasion, d'informer le public de la nouvelle situation juridique et de la possibilité du blocage des données.

3.8 Remarques particulières

3.8.1 Législation sur l'information

Comme le précisait le rapport précédent, la législation sur l'information diminue la protection des données, notamment de celles qui ne sont pas particulièrement dignes de protection. Les conséquences ne pourront être évaluées avec précision qu'après un certain laps de temps. Il est surprenant de constater, après une année, que les personnes concernées réagissent aussi de manière tout à fait positive: c'est ainsi que dans les communes ayant informé leur population dans les détails (cf. ch. 3.7), la proportion des personnes qui ont demandé le blocage de leurs données est généralement inférieure à 5 pour cent. Il y a sans doute lieu d'admettre qu'une majorité ne se préoccupe absolument pas de telles questions, mais la conclusion qui s'impose malgré tout est que les personnes concernées s'accommodent tout à fait de la communication de données pas particulièrement dignes de protection (p. ex. le fait de détenir un chien). En outre, le faible nombre des demandes de blocage témoigne sans doute aussi de ce que les personnes concernées partent du principe qu'en cas de doute, l'administration communale procédera à une pesée des intérêts avec tout le soin requis. Le bien-fondé de ce raisonnement est d'ailleurs corroboré par les nombreuses demandes émanant de services administratifs. Parmi les questions posées, certaines portaient aussi sur les inconvénients du blocage des données, par exemple dans le cas d'une réunion de classe (pas d'envoi d'invitation). Comme on pouvait s'y attendre, des tiers ont demandé à connaître le salaire de certains fonctionnaires tant cantonaux que communaux. Dans de tels cas, la pratique (encore peu abondante) recommande de communiquer le montant des traitements (sans les allocations sociales), mais conseille de consulter les intéressés au préalable. Un premier bilan plus approfondi figurera dans une brochure que la Chancellerie d'Etat projette d'éditer.

Le 23 janvier 1996

Le délégué à la protection des données: *Siegenthaler*