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): **- (2002)**

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

PDF erstellt am: **27.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-544965

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.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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

3.1 Introduction

3.1.1 2002 en bref

Face à la nécessité de réaliser des économies, l'une des réactions consiste à recourir toujours davantage aux systèmes de traitement des données, comme en témoignent des projets informatiques tels que BESIC (système commun d'informations cliniques), SYPS (système de saisie des prestations de soins), GERES (plate-forme centrale destinée aux services de contrôle des habitants) et GRUDIS (système d'information sur les données relatives aux immeubles). Si des responsables de la protection des données ont d'emblée été invités à participer aux travaux relatifs à ces projets et à en influencer le cours – avec des ressources nettement insuffisantes, il est vrai –, il n'en a pas été de même pour le projet de remplacement du système BAK (évaluation des besoins des personnes âgées résidant en institution). Le fait que l'introduction généralisée de nouveaux systèmes d'évaluation porte atteinte aux droits de la personnalité de 13000 résidents illustre le danger que recèle l'adoption, dans l'urgence, de systèmes de traitement des données sans examen des questions de protection des données.

3.1.2 Collaboration avec le préposé fédéral à la protection des données et l'association des Commissaires suisses à la protection des données, 9e Conférence suisse des commissaires à la protection des données

Sans le rapport élaboré par le groupe de travail «Santé» de l'association des Commissaires suisses à la protection des données et la liste des adaptations nécessaires qui le complétait, le Bureau n'aurait pas été en mesure de prendre position au sujet du système RAI d'évaluation des besoins des personnes résidant dans un home (cf. ch. 3.10.1). D'une part, il n'aurait pas pu consacrer le temps nécessaire à l'examen de ce système, et d'autre part, les connaissances informatiques apportées par le préposé fédéral à la protection des données lui auraient fait défaut.
La brochure intitulée «Sécurité et outils modernes de communication», mise à la disposition des membres de l'association, a pu être distribuée aux communes (cf. ch. 3.8).
Le soutien à l'élaboration de prises de position cantonales au sujet d'actes législatifs fédéraux reste une activité importante de l'association, tout comme l'organisation de cours de perfectionnement. C'est ainsi qu'à l'occasion de l'assemblée de printemps, le professeur Martin Killias a prononcé un exposé sur la poursuite pénale et la protection des données, et que les thèmes de l'introduction d'un numéro personnel d'identification au niveau fédéral (cf. ch. 3.6.2), des systèmes de reconnaissance des visages ainsi que des rapports entre la protection des données et la sécurité intérieure à la suite des attentats du 11 septembre ont été abordés lors de l'assemblée d'automne.

3.2 Description de tâches, priorités, moyens à disposition

3.2.1 Priorités

Les dossiers continuent à être traités en fonction des priorités 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. Les affaires courantes – en particulier un nombre croissant de questions posées par courriel – qui ne requièrent ni la consultation d'autres services, ni de longues recherches de la part du Bureau, sont traitées dès réception. Le problème de la longueur des délais d'attente pour les avis de droit évoqué dans les rapports annuels précédents n'a toujours pas trouvé de solution (cf. ch. 3.2.2). Enfin, faute de ressources suffisantes, aucun contrôle (inspection notamment) n'a eu lieu sans raison particulière (dénonciation à l'autorité de surveillance).

3.2.2 Recommandation de la Commission de gestion du Grand Conseil concernant l'impossibilité chronique de remplir le mandat légal de la protection des données

Comme l'indiquait le rapport précédent, le Conseil-exécutif entend remédier aux insuffisances chroniques dans l'accomplissement du mandat légal de la protection des données au moyen de transferts de tâches, sans création de postes. A la fin de l'année, la rédaction des arrêtés du Conseil-exécutif nécessaires à cet égard n'était pas encore achevée. Il s'est notamment avéré difficile de parvenir à un consensus au sujet de l'examen des projets informatiques et des activités de contrôle des applications informatiques. Au moment de l'élaboration du présent rapport, les travaux se poursuivent.

3.2.3 Responsabilité propre des services traitant des données

L'activité principale du Bureau consiste toujours à prendre position au sujet des questions que les services officiels lui soumettent. Il a été amené à examiner de nombreux projets informatiques (cf. 3.4.1). Différentes directives relatives à la protection des données ont par ailleurs été actualisées ou complétées (cliniques psychiatriques, Direction des travaux publics, des transports et de l'énergie). L'Office d'organisation a fait procéder à un audit de sécurité (cf. ch. 3.2.5).

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

Les investissements prévus dans le domaine informatique se montaient à 31 millions de francs, alors que 138 millions de francs (dont CHF 50 mio destinés à des tiers prestataires de services) devaient être consacrés à l'exploitation (montants budgétés). A cela s'ajoute que des projets importants, tels que BESIC (cf. ch. 3.4.1,

enveloppe financière supérieure à CHF 19 mio), ne figurent pas dans le budget cantonal. Quant au coût total du Bureau, il s'est maintenu à quelque 0,25 million de francs. Force est de constater que le rapport entre les montants consacrés à l'informatique d'une part et à la protection des données d'autre part reste insatisfaisant.

3.2.5 Contrôle du traitement de données informatiques

Dans son rapport de 2000, le Bureau présentait la nouvelle solution adoptée en matière de contrôle dans l'ordonnance sur l'assurance-maladie, qu'il considérait comme prometteuse: l'Office des assurances sociales et de la surveillance des fondations (OASSF), qui dispose des ressources nécessaires, est tenu de confier périodiquement à un organe indépendant le réexamen de son système de contrôle interne. Or, aucun système de contrôle interne n'a été mis en place dans le délai de deux ans prévu par le rapport accompagnant l'ordonnance, et il n'a pas davantage été fait appel à un organe de contrôle externe. S'il devait rapidement s'avérer que ces omissions ne sont que passagères, le soupçon selon lequel la disposition en question a servi avant tout d'argument facile en faveur d'un accès étendu aux données fiscales s'en trouverait invalidé.
La Police cantonale n'a pas non plus respecté – pour autant que l'on puisse en juger au moment de l'élaboration du présent rapport – l'obligation qui lui est faite, dans l'autorisation d'exploitation des systèmes d'information délivrée par le Conseil-exécutif, de charger un service indépendant de procéder à des audits. En tout état de cause, le Commandement de police n'en est qu'au stade de la mise en place d'un contrôle interne par la commission «Protection des données», alors que ce contrôle est la condition garantissant l'efficacité des audits externes.
Il n'en reste pas moins que de tels audits donnent lieu à des appréciations et à des suggestions d'amélioration qui, de l'avis même des exploitants des systèmes, revêtent une importance non négligeable. C'est en tout cas l'expérience qu'ont faite l'Office d'organisation en rapport avec BEWEB, BEMAIL et BEWAN ainsi que l'Office de l'agriculture pour l'application informatique GELAN (utilisée par les cantons de Berne, Fribourg et Soleure pour la gestion des données agricoles, en rapport notamment avec les paiements directs).
L'évaluation des risques liés à l'informatique mentionnée dans le rapport de l'année dernière, à laquelle le Contrôle des finances a procédé avec l'appui d'un service externe, a abouti à la rédaction d'un rapport transversal. Ce dernier recommande l'élargissement des normes de sécurité du plan de zones TI et l'édiction de directives cantonales sur la sécurité physique des infrastructures informatiques, deux démarches que le Bureau ne peut que soutenir (cf. ch. 3.3.1).

3.3 Sécurité des données

Les données sur papier continuent également à poser des problèmes de sécurité, comme l'illustre le fait suivant: les cliniques de médecine dentaire avaient placé des anamnèses et d'autres documents médicaux dans les conteneurs d'un centre de ramassage, et ce n'est que suite à l'intervention d'une tierce personne que ces documents ont été, le soir même, transférés en lieu sûr. Si le simple bon sens permet de prendre immédiatement conscience de l'irrégularité d'un tel procédé, il n'est généralement pas aussi aisé de déceler les risques dans le domaine de la sécurité informatique: c'est ainsi que le collaborateur d'une prison régionale, en cliquant sur la mauvaise ligne d'un répertoire d'adresses électroniques, a envoyé à un prestataire de services informatiques externe une liste nominale des détenus mentionnant les délits commis. Depuis un certain temps déjà, cette liste – non cryptée – était quotidiennement envoyée par courriel contrairement aux instructions de l'Office de la privation de liberté et des mesures d'encadrement qui considère, à l'instar du Bureau, avoir affaire en l'espèce à des données particulièrement dignes de protection qui ne sauraient être transmises par courrier électronique sans cryptage préalable. Désormais, les prisons régionales disposent, pour la saisie des listes de détenus, d'un serveur central auquel a accès le service compétent de l'office. Une solution est actuellement mise en place pour que cet accès revête également une forme cryptée. La possibilité d'un transfert des listes par télécopie avait été envisagée, mais elle s'est également avérée inadmissible. En effet, le transfert de données non cryptées n'est pas plus sûr par télécopie que par courriel. En conséquence, lorsqu'une petite unité éloignée n'a pas accès au serveur central, il convient soit de prévoir un système de cryptage des télécopies, soit de transmettre les documents par courriel sous forme de pièces jointes préalablement cryptées (cf. ch. 3.3.2). Il s'est par ailleurs agi d'attirer l'attention des services compétents de la Direction des finances sur le fait que les prestataires externes de services informatiques ne doivent désormais plus figurer dans les répertoires d'adresses électroniques cantonales. Il a enfin fallu se rendre à l'évidence: l'introduction d'un système de cryptage des courriels ne change rien au fait qu'il est toujours possible de sélectionner les mauvais destinataires.

3.3.1 Consignes

Les principales consignes en matière de sécurité informatique dans l'administration cantonale sont toujours celles de l'arrêté du Conseil-exécutif n° 4637/92 (19 mesures), tandis que l'arrêté n° 1347/98 règle l'utilisation des mots de passe. L'Office d'organisation, dans le cadre du plan de zones TI, a résumé sous forme de mots-clés, dans un tableau de trois pages, les normes de sécurité relatives au câblage des bâtiments, à l'identification des utilisateurs, à la réglementation des accès aux locaux informatiques, à la protection des locaux, à la protection contre les virus, à l'authentification et au chiffrement, à la sauvegarde des données ainsi qu'à l'alimentation électrique. A cela s'ajoute que plusieurs ordonnances renvoient à titre complémentaire, pour le domaine dont elles traitent, à la directive S 02 «Protection de base des applications et systèmes informatiques» de la Confédération. Par contre, il n'existe toujours pas de consignes détaillées, sur le modèle de la directive S 02 de l'administration fédérale (environ 260 mesures) ou du manuel allemand destiné à l'administration et à l'industrie (IT-Grundschutzhandbuch). Cette lacune est à déplorer – avis que partage le Contrôle des finances (cf. ch. 3.2.5). Il convient de rappeler en particulier que la formulation de consignes de sécurité informatique à l'intention des personnes traitant les données est exigée tant par la nouvelle loi sur la Bedag s'agissant des mandats confiés à cette dernière que par l'ordonnance sur les patients en ce qui concerne les dossiers médicaux électroniques.

3.3.2 Sécurité du courrier électronique

En matière de sécurité informatique, la question la plus fréquemment posée concerne les moyens de transmettre de manière sûre, par courriel, des pièces telles que des procès-verbaux de séances des autorités communales. Un document de travail élaboré avec la collaboration de deux préfectures expose les possibilités actuelles en la matière et les difficultés pratiques qui y sont liées. Le besoin d'un système de courrier électronique d'utilisation aisée, garantissant la confidentialité et la validité, reste pressant (cf. ch. 3.3).

3.4 Projets informatiques

3.4.1 Projets suivis par le Bureau

Le Bureau a été prié d'examiner les questions de protection des données par la direction des projets BESIC (système d'informations cliniques uniforme dans les hôpitaux et cliniques publics et subventionnés par les pouvoirs publics du canton de Berne, qui fait partie des mesures destinées à améliorer la situation professionnelle du personnel soignant APERS et dont l'enveloppe financière est supérieure à CHF 19 mio), SEP (système de saisie des prestations de soins dans les hôpitaux bernois, également un projet APERS, avec une enveloppe financière de CHF 3,95 mio), registre électronique de contrôle de l'exécution des peines et des mesures infligées aux adultes géré par l'Office de la privation de liberté et des mesures d'encadrement, ADS/RENO (système central de gestion du contenu en vue d'une exploitation standardisée de l'informatique dans les Directions et à la Chancellerie d'Etat, avec une enveloppe financière de CHF 4,815 mio), FIS 2000 (système d'informations financières: mise au point, a posteriori, d'un schéma de protection des données), HP 71: design de système pour le compte spécial PERSISKA (interface entre le système de gestion du personnel PERSISKA et FIS 2000), ELAR (archives électroniques de l'Office de la population et des migrations: élaboration d'un schéma de protection des données a posteriori), Migration Windows/Office (renouvellement de l'infrastructure informatique de base de la Direction de la santé publique et de la prévoyance sociale) et «gemeinsamer Benutzerpool IDS» (Informationsverbund Deutschschweiz, qui traite des données des utilisateurs de plus de 250 bibliothèques de Suisse alémanique). Suite à l'intervention d'une personne concernée, la Direction de l'instruction publique a été incitée à soumettre le logiciel d'administration Eco open utilisé par plusieurs écoles moyennes à un examen sous l'angle de la protection des données. (Au sujet de GERES, cf. ch. 3.6.)

3.4.2 Document de travail «schéma de protection des données»

L'intervention du Bureau dans le cadre de projets informatiques se fonde sur un document de travail d'une demi-page qui prévoit l'examen du respect des droits de la personnalité (droit de consultation, droit d'exiger une rectification des données, destruction des données, droit de blocage), de la proportionnalité des droits d'accès prévus, ainsi que des mesures envisagées en matière de sécurité informatique. Malgré sa simplicité, ce document a fait ses preuves. Les examens effectués ont en effet permis de déceler les problèmes – parfois élémentaires – suivants: classification erronée des données dans la stratégie informatique, impossibilité de détruire les données, absence de consignes de sécurité (et, partant, impossibilité d'astreindre les tiers prestataires de services à respecter de telles consignes), définition insuffisante des droits d'accès, voire inexistence de toute protection fondamentale en matière d'informatique.

3.5 Internet et cyber-administration

Dans ses directives relatives au contenu et au design des pages Internet du canton de Berne, l'Office d'information de la Chancellerie d'Etat précise que la publication sur le web de données concernant des personnes requiert le consentement de ces dernières ou l'existence d'une base légale. L'Office du personnel prépare d'ailleurs une telle base, qui figurera dans une ordonnance. Elle prévoit que les publications ne sont admissibles que si elles sont nécessaires à l'accomplissement des tâches, et règle les possibilités d'intervention des personnes concernées. Pour preuve – s'il en fallait une – de l'importance prise par la diffusion d'informations sur le web, on peut mentionner le site Internet d'un jardin d'enfants qui publie, avec l'assentiment de tous les parents concernés, des photos des enfants qui le fréquentent.
Par une modification de ses statuts, l'Université de Berne s'est dotée de la base légale nécessaire à l'envoi de communications aux étudiants par courrier électronique. A cet égard, le transfert de données particulièrement dignes de protection et de décisions relevant de la juridiction administrative n'est pas autorisé. Un compte de messagerie est attribué à chaque personne au moment de son immatriculation.
La Conférence informatique cantonale s'est posé la question, au sujet de la déclaration d'impôt électronique, du choix des certificats pour l'authentification du serveur.
(Cf. ch. 3.3.2 sur la sécurité du courrier électronique et ch. 3.6.2 au sujet du projet législatif et informatique GERES.)

3.6 Législation

3.6.1 Législation fédérale

Lors des procédures de consultation relatives à des lois fédérales, le Bureau ne prend plus position que sur la base des propositions de l'association des Commissaires suisses à la protection des données, qu'il transmet au service cantonal chargé de la coordination.

3.6.2 Législation cantonale

A l'occasion de la procédure de consultation concernant l'ordonnance GRUDIS, la proportionnalité de nouvelles possibilités d'appel a pour la première fois été examinée en détail, sur la base d'un questionnaire. Par ailleurs, il s'est notamment agi de veiller à ce qu'il n'y ait pas de chevauchements entre les bases légales de la procédure d'appel contenues dans la nouvelle loi sur le marché du travail et le droit fédéral, lui aussi en cours d'élaboration. De telles bases légales devront également être ancrées dans l'ordonnance sur les données géographiques. Pour ce dernier projet législatif, il est réjouissant de constater que l'on a fait appel au Bureau à un stade très précoce de la procédure déjà. L'évaluation des atteintes aux droits de la personnalité induites par les données géographiques et leur réglementation a toutefois mobilisé d'importantes ressources. La même remarque vaut pour la démarche de longue haleine entreprise par le groupe de travail GERES: le système informatique GERES (registres communaux) doit fournir aux communes une plate-forme, à l'échelle cantonale, pour la tenue des registres du contrôle des habitants. Les informations saisies serviront de fondement à divers systèmes cantonaux de traitement des données, et l'existence d'une base de données unitaire facilitera également les processus relevant de la cyber-administration. En tout état de cause, l'exploitation d'un tel système informatique requiert l'adoption d'une loi au sens formel (loi sur l'harmonisation des registres officiels). A cet égard, il convient de garder à l'esprit que les démarches entreprises en vue de l'introduction d'un numéro personnel d'identification au niveau fédéral pourraient avoir des répercussions sur le projet de loi cantonale. Dans le cas de GERES également, il a été fait appel très tôt au Bureau, qui s'en réjouit. Il en est d'ailleurs allé de même lors de la procédure d'élaboration de l'ordonnance sur les patients et les professionnels de la santé, qui précise en particulier que quiconque entend tenir des dossiers médicaux sous forme électronique doit garantir leur révisibilité et établir par écrit la liste des mesures de sécurité d'ordre général ainsi que des mesures complémentaires de sécurité informatique à prendre (cf. ch. 3.3.1). A cela s'ajoute qu'au sein d'une institution, l'accès aux dossiers médicaux doit être réglementé de façon à ce que le personnel ne puisse consulter que les pièces nécessaires à l'accomplissement de ses tâches. Enfin, l'externalisation du traitement des données médicales fait l'objet d'une réglementation.

La loi sur les soins hospitaliers ne prévoit plus l'organisation des hôpitaux régionaux et des hôpitaux de district sous forme de syndicats de communes. Or, seules les collectivités telles que les syndicats de communes sont tenues de se doter de leur propre autorité de surveillance en matière de protection des données. Il convient donc de définir quelle entité se chargera de leurs tâches à l'avenir. Il apparaît judicieux, en particulier, de contraindre également les hôpitaux qui n'étaient pas organisés jusqu'ici sous forme de syndicats de communes, comme l'Hôpital de l'Ile, à avoir une autorité de surveillance propre. La base légale nécessaire à l'introduction de systèmes d'évaluation des besoins des personnes âgées résidant en institution (cf. ch. 3.10.1) est l'ordonnance partiellement révisée sur les prestations complémentaires à l'assurance-vieillesse, survivants et invalidité, qui n'a pas été soumise au Bureau.
(Cf. ch. 3.5 au sujet de la modification des statuts de l'Université.)

3.7 Décisions de justice

3.7.1 Au sujet de la législation sur l'information

En rejetant un recours formé contre une décision des Archives de l'Etat, la Chancellerie d'Etat a confirmé que même un jugement pénal remontant à plus de 50 ans ne peut être consulté par une tierce personne qu'avec l'assentiment de ceux qui sont concernés (victimes, témoins), et que l'on ne saurait notamment partir du principe que ces personnes sont déjà décédées. C'est par ailleurs à juste titre que les Archives de l'Etat ont estimé que le travail requis pour recueillir les autorisations serait disproportionné, tout comme l'anonymisation complète du dossier. En conséquence, seul le droit de consulter le dispositif – rendu anonyme – du jugement a été accordé.

3.7.2 Au sujet de la législation sur la protection des données

Le droit de consultation doit être accordé aux personnes concernées lorsqu'elles pourraient prendre connaissance des mêmes informations auprès d'autres services, comme l'a confirmé le Tribunal administratif, en donnant tort à une commune, dans ses considérants relatifs à la liquidation des frais d'une procédure devenue sans objet. Il s'agissait de la consultation d'un rapport établi à l'intention de l'autorité de police locale par la Police cantonale appelée à intervenir dans un litige de voisinage.

3.8. Collectivités de droit communal

La commune de Langenthal a lancé un projet visant à doter les services d'informatique et de communication de son administration d'une protection de base étendue. La commune d'Ostermundigen a quant à elle présenté une ordonnance sur l'utilisation des auxiliaires informatiques. Le site Internet du Bureau contient certes des informations sur la protection des données dans les communes, mais il convient d'admettre que d'une manière générale, le soutien offert aux collectivités de droit communal en matière de sécurité informatique devrait être amélioré. Un premier pas, modeste, a pu être franchi dans cette direction avec la distribution de la brochure «Sécurité et outils modernes de communication» (cf. ch. 3.2.1). S'agissant de la sécurité du transfert de données par courriel, il est renvoyé au chiffre 3.3.2. Enfin, force est de constater que la proportion d'avis de droit rédigés à la demande des collectivités de droit communal est élevée.

3.9 Points abordés dans le rapport précédent

(Cf. ch. 3.2.5, 3.3.1, 3.3.2, 3.3.5)

3.9.1 ADN

C'est à juste titre que la proposition présentée par la commission consultative concernant un projet de loi sur l'exécution des peines et mesures renonce à réglementer la création d'une banque de données propre au canton sur les profils d'ADN établis à des fins de poursuite pénale.

3.10 Cas particuliers

3.10.1 Introduction de systèmes d'évaluation des besoins des personnes âgées résidant en institution (projet de remplacement du système BAK)

En 1996 déjà, le Bureau avait adressé à l'Office du médecin cantonal une prise de position au sujet d'un système d'évaluation, qui ne portait alors que sur les soins requis par les personnes résidant dans des établissements médico-sociaux. A l'époque, il doutait déjà de la proportionnalité de la collecte des données. Suite à l'intervention d'associations défendant les intérêts des personnes âgées, le groupe de travail «Santé» de l'association des Commissaires suisses à la protection des données a examiné, au cours de l'été 2002, le système d'évaluation RAI (Resident Assessment Instrument) utilisé dans plusieurs foyers pour personnes âgées de Suisse. Il est parvenu à la conclusion que ce système exige la collecte d'un nombre disproportionné de données, qu'il est opaque, qu'il transgresse le principe de la finalité (il vise, outre l'évaluation des besoins en matière de soins, la planification des soins, l'assurance de qualité et le décompte des dépenses), qu'il ne rend qu'insuffisamment anonymes les données utilisées à des fins statistiques et qu'il ne satisfait pas aux consignes en matière de sécurité des données. Dans le cadre du projet qui vise le remplacement du système BAK, utilisé jusqu'ici pour les décomptes, par un système plus moderne, le service compétent de la Direction de la santé publique et de la prévoyance sociale, soutenu par un groupe de travail, est parvenu à la conclusion qu'il convenait d'introduire de manière généralisée, dès le début 2003, soit le système RAI soit le système BESA pour les 13000 résidents des 300 établissements médico-sociaux que compte le canton de Berne. Dans les recommandations qu'il avait formulées fin août, le Bureau suggérait de stopper l'introduction du système RAI ou d'en corriger les défauts à court terme. La direction du projet a opté pour la seconde solution. Il n'est toutefois pas certain que la démarche du Bureau ait encore influencé les 68 établissements introduisant le système RAI: selon les informations reçues d'une personne concernée, les corrections proposées ne sont pas parvenues à temps aux établissements, qui se trouvaient en pleine phase préparatoire. Quant au système BESA, il n'a jusqu'ici pas été examiné sous l'angle de la protection des données. Le fait que le questionnaire d'observation contienne par exemple des rubriques visant à déterminer si un pensionnaire manifeste un intérêt sexuel amène toutefois à se demander si certains éléments, là aussi, ne posent pas problème.
L'introduction de nouveaux systèmes d'évaluation des besoins a surtout été dictée par les changements à apporter aux décomptes des frais. Dans ce contexte, il semble que l'on ait justement perdu le sens de la mesure s'agissant de la collecte de données sensibles concernant les soins. Pourtant, même en période de restrictions budgétaires, le respect des droits de la personnalité des aînés aurait exigé que les systèmes fassent l'objet, avant leur introduction, d'un examen approfondi du point de vue de la protection des données, et que les ressources nécessaires soient débloquées à cette fin.

15 janvier 2003

Le délégué à la protection des données: *Siegenthaler*