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

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

3.1 Introduction

3.1.1 2003 en bref

Le Conseil-exécutif a adopté plusieurs mesures destinées à garantir un meilleur accomplissement des tâches relevant de la protection des données. C'est ainsi que les services administratifs doivent maintenant adresser en premier lieu leurs questions en la matière à leurs services juridiques respectifs. Par ailleurs, le gouvernement peut désormais obliger les exploitants d'applications informatiques à soumettre ces dernières à un examen sous l'angle de la protection des données. Enfin, les dépenses destinées à des projets informatiques ne peuvent être décidées qu'à la condition qu'un schéma de protection des données ait été élaboré.
Les grands systèmes en réseau – tels que la plate-forme GERES qui sert, à l'échelle cantonale, à la tenue des registres du contrôle des habitants – attestent de la nécessité d'introduire de telles améliorations. Même le préposé fédéral à la protection des données n'est pas en mesure de traiter à temps les grands projets – comme l'introduction de Tarmed –, ce qui montre bien que les services responsables de la protection des données devront, à l'avenir également, se contenter de donner des impulsions.

3.1.2 Collaboration avec le préposé fédéral à la protection des données et l'association des Commissaires suisses à la protection des données

Le projet de loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes envoyé en consultation prévoit l'introduction d'un identificateur fédéral de personnes. L'association des Commissaires suisses à la protection des données demande que cet identificateur soit exclusivement utilisé à des fins statistiques, et qu'une discussion politique approfondie portant sur son principe même ait lieu au préalable. Elle a adopté lors de son assemblée de printemps une résolution à cet égard, intitulée «Le citoyen ne doit pas devenir un numéro dans la cyberadministration!». (Il est renvoyé au ch. 3.6.2 s'agissant de l'introduction d'un numéro administratif cantonal, et au ch. 3.7 à propos de la collaboration avec le groupe de travail «Santé» et le préposé fédéral à la protection des données sur les questions relevant du domaine de la santé.)

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 schémas de protection des données concernant des 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. (Le problème de la longueur des délais d'attente pour les avis de droit est traité au chiffre 3.2.2.)

3.2.2 Arrêtés du Conseil-exécutif imposant des mesures destinées à pallier l'impossibilité chronique de remplir le mandat légal de la protection des données (ACE 1102, 1103 et 1104 du 9 avril 2003)

Les services juridiques des Directions, les conseillers et conseillères en matière de protection des données le cas échéant, de même que – pour les questions en rapport avec leur domaine – les services d'informatique sont désormais les interlocuteurs des unités administratives en matière de protection des données. Eux seuls ont encore, comme les citoyens et les citoyennes, un accès direct au Bureau (cf. ch. 3.9 s'agissant des collectivités de droit communal). Lorsqu'il a adopté, au printemps, ce premier arrêté visant à décharger le Bureau, le Conseil-exécutif a pris connaissance du fait que celui-ci classerait sans les traiter tous les dossiers alors en suspens depuis plus d'une année (au nombre de 120 environ).
Le Conseil-exécutif entend, selon le deuxième arrêté, consacrer désormais environ un pour mille des frais annuels d'exploitation du parc informatique au contrôle des applications informatiques, sous l'angle de la protection des données, par des services externes. Il établira un plan indiquant les applications à contrôler ainsi que la portée précise de l'examen. C'est aux unités organisationnelles exploitant les applications qu'il appartiendra de faire appel aux organes de contrôle indépendants.
Le troisième arrêté du Conseil-exécutif adopté dans ce contexte oblige les services qui entendent solliciter une autorisation de dépense pour un projet informatique à présenter au préalable un schéma de protection des données précisant la manière dont seront respectés les consignes en matière de sécurité informatique (cf. ch. 3.3.1) et les droits des personnes concernées à la protection de leurs données (droit de blocage, droit d'exiger une rectification des données, droit de consultation, destruction des données). En outre, le schéma renseignera sur les droits d'accès et les modalités de journalisation.
Il est encore trop tôt pour évaluer les répercussions des arrêtés du Conseil-exécutif. On peut cependant d'ores et déjà relever que les services juridiques des différentes unités fournissent des conseils de qualité en matière de protection des données également, de sorte que le Bureau a bénéficié d'un allégement sensible de sa charge de travail.
Le plan d'examen des applications informatiques n'en est pour sa part qu'au stade de l'élaboration (cf. ch. 3.4.1 au sujet des schémas de protection des données.)

3.2.3 Responsabilité propre des services traitant des données

Divers exemples attestent de l'engagement considérable dont font preuve les services appelés à traiter des données: on peut citer à ce propos le projet de directive sur l'utilisation des auxiliaires informatiques par les institutions de formation du corps enseignant, l'intégration de la protection des données comme branche des cours interentreprises destinés aux apprentis ou encore l'élaboration d'un programme sur la sécurité destiné à l'application informatique GELAN (versement de contributions agricoles). Il est de plus en plus fréquent, en outre, que des maîtres de données – comme l'Intendance des impôts – examinent dans les détails, en présence de

projets d'accès à leurs propres données à partir d'autres systèmes, quel sera le traitement de ces dernières par de tels systèmes.

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 39 millions de francs, alors que 140 millions de francs (dont CHF 61 mio destinés à des tiers prestataires de services) devaient être consacrés à l'exploitation (montants budgétés). Le Conseil-exécutif a décidé d'affecter, en 2004 et au cours des années suivantes, un pour mille des frais annuels d'exploitation au contrôle des applications informatiques par des services externes (cf. ch. 3.2.2). En regard du coût total du Bureau (CHF 0,25 mio environ), ce montant est loin d'être négligeable.

3.2.5 Contrôle du traitement de données informatiques

A l'occasion des audits internes, le Contrôle des finances procède désormais à une appréciation des risques dans le domaine informatique des services concernés (interview de la personne responsable de l'informatique). Quant à la Bedag Informatique SA, qui est tenue, de par la loi sur la Bedag, de faire contrôler chaque année les points essentiels de la sécurité de l'information par un organe spécialisé externe et indépendant, elle s'est acquittée de ce mandat en demandant un audit préalable dans la perspective de la certification de sa sécurité informatique selon le British Standard BS 7799–2:2002.
(Il est renvoyé au ch. 3.2.2 s'agissant du recours à des services externes pour les contrôles à venir des applications informatiques, au ch. 3.10.4 à propos du changement intervenu dans l'obligation imposée au Commandement de la police de faire appel à des organes de contrôle externes indépendants, ainsi qu'au ch. 3.10.2 en ce qui concerne la solution adoptée en matière de contrôle par l'Office des assurances sociales et de la surveillance des fondations.)

3.3 Sécurité des données

Les schémas de protection des données concernant les projets informatiques (cf. ch. 3.2.2 et 3.4) attirent régulièrement l'attention sur des lacunes en matière de sécurité. Ainsi, le Bureau a été amené à rappeler, à propos de la sécurité des transmissions, que le Conseil-exécutif avait autorisé en 1997 le réseau cantonal de communications longues distances BEWAN pour le seul transfert de données internes ou non classées, et en aucun cas pour celui de données confidentielles ou secrètes.

3.3.1 Consignes

Dans ses arrêtés visant à réduire le volume de travail du Bureau, le Conseil-exécutif a chargé l'Office d'organisation de donner d'ici la mi-2004, d'entente avec la Conférence informatique cantonale et avec le concours du Bureau, le mandat à un ou une spécialiste de l'informatique d'établir une expertise indiquant comment développer les consignes existantes en matière de sécurité informatique. Ces dernières sont en effet insuffisantes, comme l'a révélé en particulier le traitement des schémas de protection des données qui doivent désormais impérativement accompagner les projets informatiques. Le schéma du projet FIS 2000 (système d'informations financières) précise pour sa part que des consignes détaillées et à jour devraient être développées à l'échelle cantonale en matière de sécurité informatique. Les consignes se sont par ailleurs également révélées insuffisantes lors du traitement de projets allant dans la direction de la cyber-administration (évaluation des élèves et système de disposition des dates d'expertises et d'examens de conduite: cf. ch. 3.4.1).
Il n'en reste pas moins que la directive édictée par la Conférence informatique cantonale au sujet de l'utilisation des codes d'utilisateurs montre le bon chemin, en tout cas dans un domaine précis.

3.3.2 Sécurité du courrier électronique

La Conférence informatique cantonale a adopté un avant-projet en vue de l'introduction d'une infrastructure Public-PKI et SecureMail. Il s'agit de permettre la transmission de données particulièrement dignes de protection par courriel en faisant appel aux certificats de classe 2 et aux authentifieurs «soft tokens» disponibles sur le marché. Lors de la phase d'évaluation, le Bureau a dû indiquer que ses ressources ne lui permettaient pas d'examiner les délicates questions de droit qui se posent dans ce contexte. L'avant-projet ne requiert d'ailleurs pas de solution à cet égard. Il s'agit bien plutôt de chercher à résoudre à court terme et de manière pragmatique le problème de sécurité que pose le transfert de données particulièrement dignes de protection.

3.4 Projets informatiques

Désormais, le Conseil-exécutif soumet les autorisations de dépense pour tous les projets informatiques portant sur un montant supérieur à 100 000 francs à la condition qu'un schéma de protection des données ait été établi (cf. ch. 3.2.2); ce schéma doit en outre avoir été adressé au Bureau afin qu'il prenne position. Il s'agit là d'une consigne qui améliore la prise en compte des exigences de la protection des données.

3.4.1 Projets suivis par le Bureau

Des schémas de protection des données ont été présentés par les directions de divers projets informatiques: base de données géographiques (cf. ch. 3.6.2 à propos du projet d'ordonnance), saisie des prestations avec IBIcare (en vue d'introduire un nouveau système d'enregistrement des prestations médicales), ELAR (archives électroniques de l'Office de la population et des migrations: mise à jour du schéma de protection des données élaboré a posteriori) et FIS 2000 (système d'informations financières: mise au point, a posteriori, d'un schéma de protection des données).
L'instrument qu'est le schéma de protection des données doit encore être consolidé. Le document que la direction du projet FIS 2000 a élaboré avec le concours de services externes peut toutefois servir d'exemple en la matière.
Indépendamment de la décision concernant le projet BESIC (système d'informations cliniques uniforme dans les hôpitaux et cliniques publics et subventionnés par les pouvoirs publics du canton de Berne), la Direction de la santé publique et de la prévoyance sociale a chargé un service externe d'élaborer un schéma de protection des données général pour les hôpitaux. Cette démarche, que l'on ne peut que saluer, aura toutefois des effets pervers si l'Office des hôpitaux invoque l'adoption future d'un tel schéma pour refuser – comme il l'a fait à propos de la subvention cantonale en faveur de l'hôpital régional de l'Emmental pour IBIcare – la mise en œuvre d'améliorations ponctuelles, sous l'angle de la protection des données, de projets précis.
Certaines directions de projets se sont engagées à élaborer a posteriori un schéma de protection des données; tel est le cas pour le projet «Rénovation PERSISKA» (mise à jour du système informatique du personnel, réunion et remaniement des consignes en matière de protection des données), le projet d'harmonisation concer-

nant BESIS (mise en œuvre, dans le domaine des trois cliniques psychiatriques cantonales, de l'harmonisation de l'informatique à l'échelle cantonale) et le projet «VITSek II» (informatique administrative dans les écoles du cycle secondaire du 2e degré).
L'absence de consignes cantonales en matière de sécurité se fait particulièrement sentir dans le cas de projets allant dans la direction de la cyber-administration. Le Bureau a été amené à traiter les projets «VPZ-Dispo» (système permettant aux particuliers, aux garages et aux moniteurs d'auto-école de gérer directement les dates d'expertises et d'examens de conduite par le biais d'Internet) et «Schübe» (établissement des rapports d'évaluation des élèves par le corps enseignant grâce à un serveur central mis à disposition par la Direction de l'instruction publique et accessible par le biais d'Internet, archivage des documents pendant 15 ans à compter de la sortie de l'école). Schübe n'a été soumis au Bureau que sur demande et sans schéma de protection des données. (Cf. ch. 3.6.2 à propos de GERES.)

3.5 Internet et cyber-administration

A l'instar des hôpitaux privés, certains hôpitaux publics offrent aux parents la possibilité de publier des photos de leurs enfants nouveau-nés sur un site Internet. Il s'est agi de leur rappeler que l'accord des parents ne suffit pas à pallier l'absence de base légale en la matière.
Quant à la diffusion de photos de collaborateurs et de collaboratrices – même si elle a lieu non pas sur Internet mais sur Intranet –, non seulement elle requiert une base légale, mais elle doit en outre être nécessaire à l'accomplissement des tâches (proportionnalité). Cette condition a dû être rappelée à différents services.
Enfin, plusieurs unités organisationnelles ont édicté des directives sur l'utilisation d'Internet et du courriel.
(L'absence de consignes de sécurité dans le domaine informatique pour les solutions relevant de la cyber-administration est traitée au ch. 3.4.1, et GERES au ch. 3.6.2.)

3.6 Législation

3.6.1 Législation fédérale
(Cf. ch. 3.1.2 et 3.10.1)

3.6.2 Législation cantonale

Les travaux concernant l'ordonnance sur les données géographiques se sont poursuivis (cf. également le ch. 3.4.1), tout comme l'élaboration de la loi sur l'exploitation du système informatique GERES (registres communaux). Cette loi prévoit en particulier l'introduction d'un numéro administratif cantonal. Pour examiner la question des limites constitutionnelles d'une telle réglementation, le Bureau a pu se fonder sur une expertise traitant du même objet au niveau fédéral que le professeur Giovanni Biaggini a établie sur mandat du préposé fédéral à la protection des données.

3.7 Santé

Des instruments inédits sont utilisés ou testés dans le cadre de projets pilotes pour la saisie et le décompte de prestations médicales. Il n'est pas rare, à cet égard, que l'introduction de nouvelles méthodes implique celle de nouveaux outils informatiques. C'est ainsi que le projet SEP (système de saisie des prestations de soins dans les hôpitaux bernois) évoqué dans le rapport de 2002 se fonde sur la méthode LEP de saisie des prestations de soins infirmiers. Il est par ailleurs prévu de tester la méthode APDRG (All Patient Diagnoses Related Groups) dans plusieurs hôpitaux. Enfin, le 1er janvier 2004 marque l'introduction de Tarmed (cf. ch. 3.1.1; Tarmed entraîne une transmission standardisée et systématique de données personnelles détaillées au moyen de formulaires de facturation).
L'appréciation de tels systèmes informatiques et méthodes sous l'angle de la protection des données représente un travail de longue haleine, d'une extrême complexité, qui requiert des connaissances dans les domaines de l'informatique, du droit de l'assurance-maladie ainsi que de la médecine. Comme ces systèmes et méthodes doivent le plus souvent être introduits à l'échelle nationale (législation sur l'assurance-maladie), le Bureau cherche à résoudre les problèmes qu'ils soulèvent en collaboration avec le groupe de travail «Santé» de l'association des Commissaires suisses à la protection des données et le préposé fédéral à la protection des données. Il n'en reste pas moins que les ressources ainsi réunies ne suffisent souvent même pas pour soumettre à temps ne serait-ce que l'un des instruments à un contrôle. Quant aux autres, tels que Tarmed (cf. ch. 3.1.1), il est possible de les examiner a posteriori uniquement, si tant est qu'une telle démarche entre en ligne de compte.
La complexité de l'examen du traitement des données dans le domaine médical est également illustrée par le laps de temps dont a eu besoin la commission d'experts fédérale compétente pour délivrer à l'Hôpital de l'Ile l'autorisation de lever le secret professionnel en matière de recherche médicale: la décision est en effet intervenue en 2003, soit dix ans après la date prévue par la législation.

3.8 Surveillance et décisions de justice

3.8.1 Procuration en blanc permettant à l'Office AI de Berne d'obtenir des renseignements

Toute personne sollicitant des prestations de l'assurance-invalidité doit, selon la pratique de l'Office AI de Berne, signer une procuration par laquelle elle autorise l'ensemble des personnes et services concernés – à savoir les médecins, le personnel paramédical, les hôpitaux et autres établissements de soins, les caisses-maladie, les employeurs, les avocats et avocates, les sociétés fiduciaires, les compagnies d'assurance tant publiques que privées, les services publics chargés des institutions privées d'aide sociale ainsi que les services compétents de l'assurance-vieillesse, survivants et invalidité – à fournir à l'Office AI les renseignements dont il a besoin pour l'examen et la vérification du droit aux prestations ainsi que pour l'exercice du droit de recours contre un tiers responsable. En sa qualité d'autorité de surveillance, l'Office fédéral des assurances sociales a admis un recours dirigé contre cette pratique, confirmant ainsi une prise de position que le Bureau avait adressée précédemment à l'Office AI selon laquelle une telle procuration en blanc était contraire au droit.

3.8.2 Droit des proches d'une personne décédée de consulter le dossier pénal de cette dernière

Les proches d'un inculpé décédé (en l'espèce sa mère, sa compagne et leurs enfants communs) sont habilités – en l'absence d'intérêts prépondérants au secret – à consulter le dossier de la procédure pénale dirigée contre le défunt, notamment pour des motifs relevant du droit de la personnalité. La Chambre d'accusation a en effet rendu une décision allant dans ce sens suite à un recours formé par les personnes intéressées contre la décision d'un juge d'instruction qui leur refusait l'accès au dossier.

3.8.3 Accès à la banque de données des clients titulaires de cartes d'un grand distributeur dans une procédure pénale

Si des outils achetés auprès d'un grand distributeur sont retrouvés sur le lieu d'une infraction, l'autorité d'instruction peut utiliser (avec des restrictions géographiques) la banque contenant les données des clients titulaires de cartes de ce distributeur pour établir l'identité de la personne qui a acheté les outils en présentant sa carte de client. La Chambre d'accusation a rejeté un recours formé par le grand distributeur, qui invoquait la protection de la personnalité. Elle s'est fondée, à cet égard, sur la base légale qui, dans le Code de procédure pénale, autorise le prélèvement d'informations contenues dans une banque de données informatique, et a examiné en particulier la proportionnalité de l'intervention, qu'elle a confirmée en l'espèce. Elle a par ailleurs enjoint à l'autorité d'instruction d'informer le grand distributeur de la radiation des données dans ses propres dossiers et dans ceux de la police.
Cette décision rappelle deux choses: d'une part, le recours à des auxiliaires modernes de traitement des données telles que les cartes de client permet, même après une assez longue période, de reconstituer précisément des actes quotidiens et anodins (comme l'achat d'outils), et d'autre part, il existe de ce fait des fichiers exploitables auprès de services traitant des données qui sont régis par le droit tant privé que public.

3.8.4 Vote aux urnes sur les demandes de naturalisation

(Cf. ch. 3.9)

3.9. Collectivités de droit communal

L'une des mesures destinées à pallier l'impossibilité chronique de remplir le mandat légal de la protection des données (cf. ch. 3.2.2) prévoit que les collectivités de droit communal ont pour interlocuteur l'Office des affaires communales et de l'organisation du territoire ou le service spécialisé compétent de l'administration cantonale. Les autorités communales de surveillance de la protection des données peuvent toutefois continuer de s'adresser au Bureau. Pour autant que l'on puisse en juger après une aussi brève période, la nouvelle réglementation s'avère judicieuse.
Les collectivités de droit communal sont confrontées à des questions délicates en matière de protection des données, comme celles de la compétence d'édicter une base légale autorisant la vidéosurveillance dans les transports publics (p. ex. bus) qui desservent plusieurs communes, ou encore des modalités admissibles de détermination du domicile fiscal des personnes qui séjournent à la semaine dans une commune.
L'introduction, dans les collectivités de droit communal, d'une obligation d'établir un schéma de protection des données telle qu'elle existe pour les projets informatiques du canton (cf. ch. 3.4) serait souhaitable. Cette constatation s'impose après qu'un membre d'une autorité communale a relevé que dans sa commune de taille moyenne, tous les collaborateurs et collaboratrices, quelle que soit leur fonction, avaient accès sans restriction à l'ensemble des informations.
C'est entre autres motifs pour préserver le droit fondamental à la protection des données des personnes concernées que le Tribunal fédéral a déclaré inadmissible que le peuple se prononce par la voie des urnes sur les demandes de naturalisation. Si les décisions en la matière sont prises en assemblée communale, cela signifie que les prétentions à la protection des données des personnes candidates à la naturalisation s'opposent aux prétentions à l'information des ayants droit au vote. Les propositions de ne pas accorder la naturalisation sont les premiers exemples des difficultés considérables que peut poser, dans la pratique, la pesée d'intérêts contradictoires.
S'agissant de l'application informatique Schübe qui est placée sous la responsabilité des communes, il convient de se référer au chiffre 3.4.1.

3.10 Points abordés dans le rapport précédent

(Cf. ch. 3.2.2, 3.3.1 et 3.3.2)

3.10.1 ADN

La loi fédérale sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification de personnes inconnues ou disparues a été adoptée par les Chambres fédérales vers le milieu de l'année. Une fois en vigueur, elle devra être mise en œuvre dans le canton de Berne également. Les commissaires à la protection des données, qui demandaient d'une part l'effacement d'office des données et d'autre part l'établissement d'une liste des infractions conduisant à une inscription dans la banque de données, ont obtenu gain de cause sur le premier point, mais pas sur le second.

3.10.2 Contrôles du traitement informatisé des données à l'Office des assurances sociales et de la surveillance des fondations

Un organe de contrôle externe spécialisé a été désigné en vue de l'exécution du mandat énoncé dans l'ordonnance sur l'assurance-maladie, qui oblige l'office à mettre en place un système de contrôle interne et d'en confier périodiquement le réexamen à un organe indépendant.

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

Le système d'évaluation des besoins des personnes âgées résidant en institution RAI/RUG, qui implique un traitement de données disproportionné, est actuellement remanié par le fournisseur. Quant au système BESA, il est désormais disponible dans une nouvelle version. Après examen de son schéma de protection des données, le délégué à la protection des données du canton de Zurich a relevé que des améliorations étaient patentes. Ce même délégué entend examiner également le schéma de protection des données du système RAI/RUG. S'il s'avère que les corrections nécessaires ont été apportées dans les deux cas, il s'agira, dans le canton de Berne, de procéder au remplacement des systèmes utilisés jusqu'ici. Tant que cette démarche n'a pas eu lieu, et malgré les améliorations introduites, on ne saurait admettre que toutes les exigences sont respectées.

3.10.4 Autorisation d'exploiter les systèmes de traitement des données de la Police cantonale

Dans son arrêté imposant le réexamen d'applications informatiques (cf. ch. 3.2.2), le Conseil-exécutif a indiqué que les systèmes de traitement des données de la Police cantonale devraient eux aussi être contrôlés conformément au plan qu'il doit encore élaborer. Ce faisant, il a prolongé d'une part le délai imparti pour le premier examen par un organe de contrôle externe, et supprimé d'autre part l'obligation de donner tous les deux ans à un organe spécialisé indépendant le mandat de s'assurer que la protection et la sécurité des données sont garanties. Ce n'est que sur la base de plusieurs plans d'examen consécutifs qu'il sera possible de dire si l'option choisie conduit à un renforcement ou au contraire à une réduction de la portée des contrôles.

Les autorisations d'exploiter concernant la centrale des amendes d'ordre et la banque de données de la Brigade «recherche de personnes» ont été soumises au Bureau sous forme de projets seulement.
Dans son autorisation d'exploiter de janvier 2001, le Conseil-exécutif avait exigé du Commandement de la police que les accès (lecture) au sous-système OBORA soient journalisés. Dans le rapport accompagnant son arrêté, il avait fixé à cet égard un délai à fin 2002. Or, au moment de la rédaction du présent rapport, les accès ne sont toujours pas journalisés. Selon les indications fournies par le Commandement de la police, la réalisation interviendra en 2004.

3.11 Cas particuliers

3.11.1 Enregistrements vidéo dans les prisons

Le rapport établi par un expert chargé d'enquêter dans les prisons régionales de Berne et de Thoune sur d'éventuelles violations du droit du personnel et irrégularités commises dans l'exploitation soulignait la nécessité de veiller à ce que les installations de vidéosurveillance des prisons ne soient pas détournées à des fins de surveillance du personnel. Les recherches auxquelles a ensuite procédé la direction de l'Office de la privation de liberté et des mesures d'encadrement ont révélé que des images étaient non seulement retransmises sur des moniteurs, mais également enregistrées. Or, de tels enregistrements ne sont autorisés qu'à condition qu'il existe une base légale. Tel n'était pas le cas en l'espèce, de sorte que la direction de l'office les a interdits avec effet immédiat. En ce moment, l'office examine s'il existe des besoins en matière d'enregistrement vidéo et lesquels, de même que la manière d'ancrer une telle mesure dans la législation.

3.11. 2 Banque de données de la Conférence suisse des directeurs cantonaux de l'instruction publique sur les enseignants et enseignantes privés de l'autorisation d'enseigner

Au cours de l'automne, la Direction cantonale de l'instruction publique a indiqué à la Conférence suisse des directeurs cantonaux de l'instruction publique (CDIP) qu'elle doutait fortement de la légalité de la banque de données que cette dernière envisage de créer sur les enseignants et enseignantes qui se sont vu retirer leur autorisation d'enseigner. Pour le Bureau, il est évident qu'une telle banque de données ne peut être instituée qu'à condition d'être prévue dans une loi au sens strict, et qu'en l'absence de dispositions légales en la matière, il est interdit aux écoles bernoises de communiquer des données destinées à son alimentation. Or, la base légale fait défaut. Il est donc pour le moins étonnant que la CDIP ait voulu faire inscrire la banque de données dans le registre des fichiers du canton de Berne. Il s'est agi de l'informer du fait que le Bureau pour la surveillance de la protection des données du canton de Berne n'assume aucune fonction de surveillance à son égard et qu'une inscription dans le registre est par conséquent exclue.

7 janvier 2004

Le délégué à la protection des données: *Siegenthaler*