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): **- (2004)**

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

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-544937

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

3.1 Introduction

3.1.1 2004 en bref

Le contrôle des applications informatiques par des tiers sous l'angle de la protection des données répond à une nécessité, comme l'illustrent les propos tenus par le médecin cantonal peu avant son départ à la retraite, lors de l'entretien final qui a eu lieu avec une représentation de son office: il a en effet déclaré n'avoir été véritablement en mesure d'assumer ses responsabilités en matière de conduite que depuis qu'un tel contrôle existe. Le Conseil-exécutif a enjoint à trois autres unités administratives de se soumettre à un contrôle par des services externes.
Les consignes en matière de sécurité informatique ne répondent plus aux besoins et doivent dès lors être développées. Cette constatation formulée par l'expert mandaté a incité le Conseil-exécutif à donner à l'Office d'organisation le mandat de les remanier d'ici la fin de 2005.

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

La Police cantonale bernoise enregistre à l'intention de tous les corps de police suisses les informations relatives aux infractions contre l'intégrité sexuelle et aux homicides, élucidés ou non, dans la banque de données du système ViCLAS qui doit permettre d'identifier la «signature» des auteurs récidivistes et d'établir leur culpabilité. La Police cantonale exploite le système ViCLAS d'entente avec la Conférence des commandants des polices cantonales de Suisse, à laquelle l'association des Commissaires suisses à la protection des données a indiqué qu'elle soutenait l'introduction d'une banque de données à l'échelle nationale à la condition qu'elle repose sur une base légale, par exemple un concordat. (Il est renvoyé au ch. 3.7.2 s'agissant de la collaboration avec le groupe de travail «Santé» et le préposé fédéral à la protection des données sur les questions touchant à Tarmed, au ch. 3.7.3 concernant la méthode APDRG, au ch. 3.6.1 pour ce qui est des prises de position cantonales par rapport aux actes législatifs fédéraux et au ch. 3.9.4 à propos de la liste des enseignants auxquels a été retiré le droit d'enseigner.)

3.2 Description de tâches, priorités, moyens à disposition

3.2.1 Priorités

Les dossiers sont traités en fonction des priorités suivantes: 1) les schémas de protection des données concernant des projets informatiques, 2) le suivi des mandats confiés à des services de contrôle externes, 3) la législation générale plutôt que la législation spéciale, 4) les directives générales plutôt que les cas particuliers, 5) les conseils et l'instruction, 6) les problèmes concernant un grand nombre de personnes plutôt que ceux touchant quelques rares individus et risquant peu de se reproduire.
Le projet EVENTO d'informatique administrative pour les écoles moyennes (cf. ch. 3.4.1) a impliqué d'examiner, lors du traitement du schéma de protection des données, si les droits d'accès aux champs de données, dont le nombre est supérieur à 200, avaient été correctement attribués en fonction des différents rôles, de plus de 30 au total. Or, un tel examen représente une charge de travail considérable. Ce cas particulier illustre de manière exemplaire les problèmes que pose le suivi des schémas de protection des données, qui se heurte à l'insuffisance des ressources. D'ailleurs, l'arrêté du Conseil-exécutif imposant de tels schémas partait du principe que le manque de ressources se ferait sentir. Il prévoyait donc la possibilité de prendre une décision en l'absence de rapport d'examen s'il s'avérait impossible de procéder à une vérification avant l'arrêté de dépense. Dans la pratique toutefois, cette possibilité se révèle de peu d'utilité, tant il est vrai que les schémas de protection des données ne sont régulièrement soumis au Bureau dans leur teneur définitive qu'une fois que le Conseil-exécutif a arrêté sa décision. Il n'en reste pas moins que les responsables de projets attendent une prise de position au sujet des schémas remaniés également.

3.2.2 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 données personnelles par les institutions de formation du corps enseignant, ou encore les recherches menées par l'Intendance des impôts à propos du questionnaire sur les frais liés à un handicap. (Cf. ch. 3.2.4 s'agissant de la certification de la sécurité informatique obtenue par la Bedag Informatique SA.)

3.2.3 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 40 millions de francs, alors que 149 millions de francs (dont CHF 64 mio destinés à des tiers prestataires de services) devaient être consacrés à l'exploitation (montants budgétés). Une somme de 130 000 francs était en outre disponible pour le contrôle des applications informatiques par des services externes (cf. ch. 3.2.4). Par ailleurs, l'Office d'organisation a financé une expertise sur le développement des consignes existantes en matière de sécurité informatique (cf. ch. 3.3.1). La Direction de la santé publique et de la prévoyance sociale, pour sa part, a débloqué des ressources importantes en faveur de l'élaboration d'un schéma de protection des données général pour les hôpitaux, dans le cadre du projet BESIC+ (cf. ch. 3.7.1). A cela s'ajoute que les dépenses destinées aux projets informatiques incluent désormais les charges liées à l'établissement des schémas de protection des données. Enfin, les conseils relatifs à la protection des données qui sont dispensés aux communes et aux unités administratives par les services juridiques spécialisés compétents entraînent également l'affectation de moyens à la protection des données. Ainsi, d'une manière générale, le rapport entre les ressources consacrées à l'informatique d'une part et à la protection des données d'autre part s'est quelque peu amélioré.

3.2.4 Contrôle du traitement de données informatiques

Une unité administrative chargée par le Conseil-exécutif de confier à des tiers le contrôle de ses applications informatiques sous l'angle de la protection des données est tenue de préciser le mandat dans un contrat écrit respectant les conditions générales de la Conférence suisse sur l'informatique. De plus, le contrat doit être soumis à l'approbation du Bureau avant sa conclusion. Le Conseil-exécutif fixe l'objet du contrôle dans son plan d'examen. Un contrôle intégral doit englober la protection des données (bases légales, proportionnalité des droits d'accès, respect des droits des personnes concernées), la sécurité informatique et l'organisation de la protection des données. Le mandat ne peut être accordé qu'à des services externes indépendants et qualifiés (connaissances dans les domaines de l'informatique, du droit et de la révision). Il convient par ailleurs d'attirer leur attention sur le caractère officiel de leur mandat, qui les soumet à l'obligation de garder le secret. C'est à eux qu'il incombe d'établir le programme de l'examen. Pour procéder aux contrôles, ils peuvent entendre les membres du personnel, consulter les documents, demander une démonstration des applications et accéder aux auxiliaires informatiques. Le «piratage éthique» leur est permis. Au terme de leur examen, les services mandatés établissent un rapport de contrôle contenant des recommandations quant aux améliorations envisageables. Le rapport – dont une copie sera remise au Bureau – doit faire l'objet d'un exposé oral. Telles sont les conditions fixées au cours de l'été par le Conseil-exécutif qui, dans un autre arrêté, a adopté le plan d'examen pour l'exercice (cf. ch. 3.1.1).

A l'Office du médecin cantonal, l'examen des banques de données et de l'environnement Windows/Office a révélé des possibilités d'améliorer la sécurité informatique ainsi que la gestion des droits d'accès, tandis que dans le cas de l'application JABIS concernant le domaine de la chasse (administration des autorisations, contrôle des peines et des mesures, statistique), c'est l'ancrage dans la législation qui doit être renforcé. L'Office de gestion et de surveillance de la Direction de la justice, des affaires communales et des affaires ecclésiastiques a soumis son système Tribuna (contrôle des affaires des tribunaux) à un examen partiel, centré sur la radiation des données. Il s'est avéré à cette occasion qu'il n'existe pas de règles en la matière et que les inscriptions concernant des amendes de peu d'importance ne sont pas effacées, de sorte qu'elles peuvent être consultées en cas de nouvelle procédure pénale, ce qui est à la fois inadmissible et contraire au droit fédéral. Au moment de la rédaction du rapport, l'examen auquel le Commandement de la police devait soumettre la centrale des amendes d'ordre n'était pas encore achevé.

Le premier bilan tiré de la nouvelle procédure montre qu'il a été possible de trouver des services qualifiés en nombre suffisant. Il n'en reste pas moins que l'attribution et le suivi des mandats sont très exigeants pour les unités administratives concernées, qui ont fait preuve d'un grand engagement tout en se montrant très ouvertes aux propositions d'amélioration (cf. ch. 3.1.1).

A l'occasion des audits internes, le Contrôle des finances a poursuivi son appréciation des risques dans le domaine informatique des différents services.

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, s'est acquittée de ce mandat en demandant un audit de certification de sa sécurité informatique selon le British Standard BS 7799-2: 2002. L'obtention de la certification montre bien à quel point cette société prend la sécurité des données au sérieux.

3.3 Sécurité des données

3.3.1 Consignes

Le spécialiste qui a reçu le mandat d'établir une expertise indiquant comment développer les consignes existantes en matière de sécurité informatique propose les démarches suivantes: une analyse de l'information et de la protection des données doit désormais permettre, pour chaque projet informatique, d'établir s'il implique le traitement de données sensibles. Dans l'affirmative, il conviendra de faire appel au Bureau quel que soit le coût du projet ainsi que d'établir un schéma de protection des données et de sécurité de l'information. De plus, une personne responsable de la protection des données et de la sécurité de l'information devra impérativement être désignée, et les deux domaines en question feront partie intégrante du contrôle de la qualité. Par ailleurs, le système ne pourra être mis en service que si les garanties sont jugées suffisantes à cet égard. Le rapport de clôture du projet devra également être remis au Bureau. Les exigences minimales en matière de sécurité des données ainsi que le plan de zones TI devront être complétés par un arrêté du Conseil-exécutif, voire une ordonnance, s'agissant des aspects suivants: amélioration de la classification des systèmes, définition de mesures contraignantes – tant organisationnelles que techniques – destinées à assurer la protection de base, revalorisation de l'analyse des risques. Cette dernière devra servir de fondement aux mesures allant au-delà de la protection de base qui se révéleront nécessaires. Le spécialiste suggère en outre d'améliorer la formation des responsables de projets et de leurs collaborateurs en matière de protection des données et de sécurité de l'information, ainsi que d'adapter à HERMES 2003 les instructions relatives au déroulement de projets informatiques. Le Conseil-exécutif a tenu compte de ces propositions et donné mandat à l'Office d'organisation de les mettre en œuvre d'ici à la fin de 2005 (cf. aussi ch. 3.1.1). Les futures consignes en matière de sécurité informatique permettront de définir le niveau de sécurité devant être garanti dans les contrats passés avec la Bedag Informatique SA, conformément aux exigences énoncées par loi sur la Bedag. A l'instar de l'administration du canton de Zurich, l'Office d'organisation élabore des conditions générales sur la sécurité de l'information et la protection des données qui devront être respectées lors de la fourniture de services informatiques.

3.3.2 Sécurité du courrier électronique

La Conférence informatique cantonale a décidé de développer une première installation permettant de tester l'infrastructure SecureMail (qui recourt aux certificats de classe 2 et aux authentifieurs «soft tokens» disponibles sur le marché), afin de disposer d'une base décisionnelle en vue d'une introduction ultérieure. L'exploitation d'un système de courrier électronique sûr implique la mise en place d'une infrastructure susceptible de générer et de distribuer des clés publiques et des clés privées (infrastructure dite ICP ou PKI). Comme la Confédération s'emploie actuellement à créer des infrastructures ICP, notamment pour que les services cantonaux puissent disposer d'un accès sûr aux applications fédérales, la Conférence informatique cantonale a estimé qu'une décision définitive quant à l'introduction de SecureMail ne pourrait intervenir que lorsqu'il serait possible d'apprécier la situation prévalant au niveau fédéral (compatibilité). (Cf. ch. 3.5 au sujet du virus Sober.I).

3.4 Projets informatiques

La consigne du Conseil-exécutif selon laquelle les demandes d'autorisation de dépense pour tous les projets informatiques portant sur un montant supérieur à 100 000 francs doivent impérativement être accompagnées d'un schéma de protection des données n'est

pas encore respectée de manière systématique. C'est ainsi que les subventions destinées à l'infrastructure informatique du centre hospitalier de Bienne ou encore au système d'information radiologique de l'hôpital d'Interlaken ont été accordées en l'absence d'un tel schéma. Le Bureau entend donc s'employer, en collaboration avec l'Office des hôpitaux, à garantir le respect de la consigne précitée lors de projets futurs.

3.4.1 Projets suivis par le Bureau

Des schémas de protection des données ont été présentés par les directions de divers projets informatiques: EVENTO (anciennement VITSek II, cf. ch. 3.2.1 et 3.5), eSVReg/GINA NT 2 (registre informatisé de l'exécution des peines et système d'administration des personnes détenues), «Renouvellement PERSISKA» (système informatique d'administration du personnel cantonal) et BESIS II (mise en œuvre, dans le domaine des cliniques psychiatriques, de l'harmonisation de l'informatique à l'échelle cantonale).
Une analyse de l'information et de la protection des données a été soumise au Bureau pour le projet ZEUS (faits d'état civil et statistiques). Ce document souligne la nécessité d'établir un schéma de protection des données.
Par ailleurs, le programme sur la sécurité a été achevé pour le projet RENO d'harmonisation de l'informatique dans l'administration cantonale. Ce programme, tout comme le schéma de protection des données du projet BESIS II, illustre bien le degré de complexité atteint par l'environnement informatique du canton de Berne. C'est ainsi que dans le cas de BESIS II, il s'est agi d'examiner si les différentes unités administratives avaient bien adopté les réglementations imposées par RENO, tandis que ce dernier projet a impliqué de s'assurer que le recours à un sous-traitant satisfaisait aux exigences de sécurité élevées qu'impose le traitement de données par des cliniques psychiatriques.
Bien que d'un coût inférieur à 100 000 francs, le projet eAutoindex a été soumis au Bureau par l'Office de la circulation routière et de la navigation. Ce projet doit permettre aux compagnies d'assurance d'accéder par le biais d'Internet aux données de leurs assurés détenteurs de véhicules, et une telle possibilité d'appel a dû être ancrée dans une ordonnance. Comme l'entreprise sous-traitante a son siège dans la principauté du Lichtenstein, des données personnelles sont traitées à l'étranger. Quant à l'idée de permettre aux particuliers d'accéder aux données concernant les détenteurs de véhicules, elle a été abandonnée. (Cf. ch. 3.2.1 s'agissant de l'insuffisance des ressources pour le traitement des schémas de protection des données).

3.5 Internet et cyber-administration

La direction du projet informatique EVENTO (cf. ch. 3.4.1) a renoncé pour l'instant à permettre aux membres du corps enseignant d'inscrire les notes dans les bulletins des élèves par le biais d'Internet en raison de l'impossibilité de garantir une sécurité suffisante au stade actuel des travaux. (Cf. ch. 3.4.1 à propos du projet eAutoindex.)
Vers la fin de l'année, le virus Sober.I a amené les responsables de l'informatique à avertir les destinataires de l'administration cantonale qu'ils cesseraient provisoirement d'être informés de l'arrivée de courriels contaminés. Plus de onze pour cent de tous les messages entrants étaient infectés par ce virus, et pour certains utilisateurs, une proportion nettement supérieure à la moitié des courriels reçus consistait en annonces de virus. De l'avis du Bureau, la mesure était donc justifiée.

3.6 Législation

3.6.1 Législation fédérale

Le Bureau a systématiquement renvoyé les instances cantonales à la prise de position de l'association des Commissaires suisses à la protection des données au sujet de la réforme des chemins de fer 2 (et en particulier de la vidéosurveillance dans les trains), de la loi fédérale sur les identificateurs sectoriels de personnes (loi SPIN) et de l'ordonnance sur les profils d'ADN (cf. ch. 3.9.1).

3.6.2 Législation cantonale

Les travaux concernant l'ordonnance sur les données géographiques se sont poursuivis. Outre divers préavis sur des dispositions isolées (p. ex. eAutoindex, cf. ch. 3.4.1), le Bureau a collaboré à la révision de l'ordonnance GRUDIS.

3.7 Santé

3.7.1 Système bernois d'informations cliniques (BESIC+)

Le Grand Conseil a rejeté le projet de système d'informations cliniques uniforme pour tous les hôpitaux publics du canton de Berne (BESIC) en enjoignant à la Direction de la santé publique et de la prévoyance sociale d'élaborer des systèmes décentralisés (BESIC+). Sur mandat de l'Office des hôpitaux, un service externe a alors établi un schéma de protection des données général pour les hôpitaux (cf. aussi ch. 3.2.3). Ce schéma représente une base essentielle non seulement en vue de l'élaboration décentralisée du projet, mais aussi, d'une manière générale, pour la protection des données en milieu hospitalier.

3.7.2 Tarmed

Dans son rapport consacré à Tarmed, le préposé fédéral à la protection des donnés a conclu que le traitement systématique de données personnelles tel que prévu est disproportionné, tant il est vrai que les assureurs n'ont pas besoin de l'ensemble des données se rapportant à une personne pour l'accomplissement de chacune de leurs tâches. Il a par ailleurs relevé que la loi oblige les assureurs à adopter un règlement de traitement. D'une manière générale, il s'est avéré que le traitement des données des assurés selon les modalités introduites par Tarmed peut compromettre le droit des patients à la protection de leurs données.
Le Bureau a rédigé en collaboration avec le groupe de travail «Santé» de l'association des Commissaires suisses à la protection des données des recommandations à l'attention de tous les hôpitaux publics, en leur proposant d'informer les patients de la situation concernant les décomptes, de n'adresser qu'au médecin-conseil les décomptes selon Tarmed débordant le cadre normal, de refuser dans un premier temps toute communication systématique des codes de diagnostic aux assureurs et de ne les fournir que sur demande, au cas par cas, et pour autant que cela soit proportionné.

3.7.3 APDRG

D'entente avec l'Office des hôpitaux, l'Hôpital de l'Ile ainsi que les hôpitaux de Thoune et d'Aarberg testent actuellement la méthode APDRG (All Patient Diagnoses Related Groups) pour les décomptes destinés aux assurances-accidents, à l'assurance militaire et à l'assurance-invalidité (décomptes selon 641 forfaits correspondant

chacun à une pathologie). Interrogé au préalable par l'Office des hôpitaux sur l'admissibilité d'un tel essai, le préposé fédéral à la protection des données a relevé qu'il n'existait pas de base légale aux décomptes selon la méthode APDRG, et que si cette dernière était employée sans l'assentiment des patients, cela constituait une violation du secret de fonction et du secret médical. L'Office des hôpitaux a malgré tout autorisé la phase de test en indiquant que la méthode en question était également appliquée dans d'autres cantons. Il envisage à cet égard des pourparlers avec la Commission des tarifs médicaux et le préposé fédéral.

3.8 Collectivités de droit communal

Les collectivités de droit communal se renseignent de plus en plus fréquemment sur les conditions légales d'une vidéosurveillance du domaine public, et il est possible de les renvoyer à cet égard aux rapports publiés sur Internet par les cantons de Bâle-Campagne et de Zurich. En tout état de cause, un enregistrement vidéo présuppose une base légale dans un règlement communal. Par ailleurs, les particuliers sont toujours plus nombreux à surveiller eux aussi le domaine public à l'aide de caméras vidéo. La Direction des travaux publics, des transports et de l'énergie a répondu par la négative à la question de savoir si la loi sur la construction et l'entretien des routes permet aux communes de se prémunir contre une telle démarche par le biais d'une décision.
La commune de Langenthal a élaboré une stratégie globale de sécurité informatique. Enfin, un document publié sur Internet, à savoir le programme de la fondation InfoSurance pour les PME, peut désormais être indiqué comme référence aux petites et moyennes communes ayant des questions en relation avec les mesures de sécurité qu'il leur incombe de prendre.
(S'agissant de la surveillance des télécommunications, cf. ch. 3.10.2).

3.9 Points abordés dans le rapport précédent
(Cf. ch. 3.7.2 et 3.7.3)

3.9.1 ADN

La loi fédérale sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues ainsi que son ordonnance d'application sont entrées en vigueur au début de 2005 (cf. ch. 3.6.1). Ces actes législatifs exigent que les données soient détruites d'office. Une ordonnance cantonale doit encore préciser les canaux de communication.

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

Le Conseil-exécutif a délivré une autorisation d'exploiter concernant la centrale des amendes d'ordre. Dans le cas de la banque de données de la Brigade «recherche de personnes» par contre, un tel document n'existe toujours qu'à l'état de projet. L'exigence d'une journalisation des accès (lecture) au sous-système OBORA formulée dans l'autorisation d'exploiter de janvier 2001 sera respectée à partir de 2005, avec deux ans de retard.
Aucun schéma de protection des données n'est nécessaire pour le système informatique de surveillance à distance, par caméras numériques, des signaux lumineux (respect des feux rouges) et des limitations de vitesse qui a été adopté par le Conseil-exécutif à l'intention du Grand Conseil. Les conditions relatives à la protection des données devront en effet être fixées dans l'autorisation d'exploiter. Il en va de même du projet informatique Metamorphose du DETEC; dans ce contexte, le Conseil-exécutif a autorisé un accès en ligne à la banque de données du Service des tâches spéciales du DETEC, auquel incombe la surveillance de la correspondance par poste et télécommunication. Simultanément, l'acquisition de postes de travail dotés d'appareils d'écoute ainsi que de graveurs de DVD a été acceptée. En vertu des nouvelles prescriptions de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication, les enregistrements des conversations restent aux mains de la police pendant la longue période de conservation qui prévaut pour les données liées à des poursuites pénales. Or, cette disposition concerne aussi les enregistrements d'entretiens avec des personnes totalement étrangères aux procédures. Il conviendra donc de réglementer les accès à de telles données avec un soin tout particulier. (Cf. ch. 3.1.2 au sujet de la banque de données ViCLAS).

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

Un recours en la matière formé selon la procédure ordinaire devant le Tribunal administratif a incité l'Office fédéral des assurances sociales à reconsidérer sa décision – mentionnée dans le rapport de 2003 – qui constatait le caractère illégal des procurations en blanc. Le Tribunal administratif n'a pas encore statué.

3.9.4 Liste des enseignants auxquels a été retiré le droit d'enseigner de la Conférence suisse des directeurs cantonaux de l'instruction publique

La Conférence suisse des directeurs cantonaux de l'instruction publique (CDIP) a proposé aux cantons de mettre à profit la modification d'un concordat pour y ancrer l'existence d'une telle liste, tenant ainsi compte des objections formulées par l'association des Commissaires suisses à la protection des données. Dans le canton de Berne, une base légale doit en outre être créée à cet égard dans la loi sur le statut du personnel enseignant.

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

L'office a engagé une procédure de certification visant l'obtention du label GoodPriv@cy afin de respecter le mandat énoncé dans l'ordonnance sur l'assurance-maladie, qui l'oblige à mettre en place un système de contrôle interne et d'en confier périodiquement le réexamen à un organe indépendant.

3.10 Cas particuliers

3.10.1 Droit d'accès provisoirement trop étendu des communes à l'application informatique IS-NESKO de l'Intendance cantonale des impôts

Entre 2002 et 2003, l'Intendance des impôts a donné aux quelque 370 communes affiliées un accès sans restriction au système d'information IS-NESKO, soit un accès étendu à l'ensemble du territoire cantonal, car il n'était techniquement pas possible de ne l'accorder qu'aux 27 centres de saisie Impôts créés à ce moment-là et aux 18 communes nouvellement compétentes en matière de remises d'impôts. Ainsi, les possibilités d'interrogation étaient disproportionnées, en particulier pour les petites et moyennes communes qui disposaient, pour l'accomplissement de leurs tâches, de données excédant largement leurs besoins. Cependant, aucun détail

n'était disponible sur les données de taxation (comme le revenu et la fortune imposables). Au début de 2005, l'application IS-NESKO sera transposée dans le système TaxCellence qui permettra quant à lui d'imposer les restrictions géographiques nécessaires. Il est toutefois prévu que les données du registre (comme l'adresse, l'état civil, la profession, la structure familiale, la confession lorsque celle-ci joue un rôle en matière fiscale) restent accessibles à l'échelle cantonale avec le système TaxCellence également, ce qui présente en particulier un avantage pour la saisie des données concernant les propriétaires fonciers domiciliés en dehors de la commune. L'admissibilité de cette solution est actuellement à l'examen, et il s'agira également de déterminer, le cas échéant, si des conditions plus précises doivent être fixées (p. ex. journalisation des accès et sanctions en cas d'abus).

3.10.2 Surveillance de la correspondance par télécommunication dans les réseaux cantonaux à des fins de poursuite pénale

La loi fédérale sur la surveillance de la correspondance par poste et télécommunication précise que seul le Service des tâches spéciales du DETEC est compétent en matière de surveillance. Le canton de Berne met son réseau de communications longues distances BEWAN à la disposition des communes et joue de ce fait le rôle de fournisseur d'accès. Par conséquent, les organes de police et de justice pénale du canton de Berne ne peuvent pas ordonner directement des mesures de surveillance – en soi internes – portant sur le réseau cantonal, mais doivent agir par l'intermédiaire du Service des tâches spéciales.

3 janvier 2005

Le délégué à la protection des données: *Siegenthaler*