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 ...

Herausgeber: Staatskanzlei des Kantons Bern

Band: - (1999)

Heft: [2]: Rapport de gestion : rapport

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

Autor: Siegenthaler

DOI: https://doi.org/10.5169/seals-544924

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

3.1 Introduction

3.1.1 1999 en bref

Le Bureau a été amené à plusieurs reprises à examiner de manière détaillée les normes applicables au traitement des données ADN. Si le débat s'est d'abord focalisé sur la création d'une banque de données ADN cantonale à des fins de poursuite pénale, il s'est rapidement élargi suite à l'élaboration d'un projet de loi fédérale sur l'analyse génétique humaine et au dépôt de nombreuses interventions au parlement cantonal. Le projet de directives sur la protection de la personnalité et des données à l'Institut de médecine légale a souligné la nécessité d'une approche globale des questions liées au patrimoine génétique. La diversité des opinions émises à l'occasion de la procédure de consultation sur le projet de modification du Code de procédure pénale (base légale pour la création d'une banque de données ADN à des fins d'identification judiciaire) témoigne du vif intérêt que cette question suscite dans le public.
Le projet de loi fédérale sur les documents d'identité des ressortissants suisses et l'avant-projet de modification du Code civil suisse concernant la tenue informatisée des registres de l'état civil (registre central à l'échelle suisse) prévoient un accès, à des fins policières, à la banque centrale de données devant être instaurée dans chacun des deux cas. Or, tant la centralisation que l'accès en ligne à des fins policières sont des questions délicates du point de vue de la protection des données. A cet égard, la pesée des intérêts exige que la procédure législative soit transparente.

3.1.2 Collaboration avec le préposé fédéral à la protection des données, sixième Conférence suisse des commissaires à la protection des données

Nombreux sont les services cantonaux qui mettent en œuvre le droit fédéral. Etant donné que les constatations des organes cantonaux chargés de veiller au respect de la protection des données peuvent avoir des répercussions sur les consignes fédérales (actes législatifs, directives, formulaires), il est judicieux que le suivi des services cantonaux soit assuré par le préposé fédéral et le Bureau travaillant de concert; d'ailleurs, la loi fédérale sur la protection des données prévoit une telle coopération sous la forme d'une assistance offerte par le préposé fédéral. Le délégué cantonal et le préposé fédéral ont effectué ensemble une visite auprès d'un office régional de placement et une autre auprès de l'Office AI de Berne, qui procède à une analyse des processus dans un domaine partiel. Les opinions émises à l'occasion de la sixième Conférence suisse des commissaires à la protection des données confirment qu'avec sa législation sur l'information du public, le canton de Berne suit la bonne direction.

3.2 Description des 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 qui ne requièrent ni la consultation d'autres services, ni de longues recherches de la part du Bureau, sont traitées dès réception. S'agissant des affaires peu prioritaires, les délais ne respectent pas les consignes légales; c'est ainsi qu'une commune a été informée, 17 mois après avoir soumis une affaire au Bureau, qu'elle était passée du 80e au 40e rang sur la liste d'attente. Si les ressources ne sont pas augmentées, il y a lieu de craindre que de telles affaires ne puissent même plus être traitées. Cette situation est encore aggravée par la complexité croissante des questions, tant il est vrai que ces dernières appellent bien plus, désormais, que la simple communication d'informations générales.
Dans une comparaison intercantonale (superficielle) des ressources, le canton de Berne devrait certes continuer à figurer dans le premier tiers. Il n'en ira cependant pas forcément de même à l'avenir, car les autres cantons ne cessent de renforcer leurs organes chargés de veiller au respect de la protection des données. Ainsi, celui du canton de Zurich est doté de 415 pour cent de postes, et celui de la ville de Zurich de plus de 200 pour cent de postes.

3.2.2 Responsabilité propre des services traitant des données

Comme jusqu'ici, l'activité du Bureau a essentiellement consisté à prendre position au sujet de questions émanant des services officiels. Les services traitant des données ont demandé davantage de cours de perfectionnement qu'en 1998. Il reste par ailleurs vrai que l'attitude des cadres par rapport aux questions de protection des données varie fortement d'une personne à l'autre. A cet égard, l'intérêt manifesté au plus haut niveau pour les questions relatives au traitement des données ADN a eu l'effet d'un détonateur. Le grand nombre de projets informatiques soumis au Bureau, l'engagement dont les Services psychiatriques universitaires ont fait preuve pour édicter des directives sur la transmission de données et les recherches effectuées par la Direction de l'instruction publique s'agissant de l'utilisation d'Internet à l'école sont autant d'éléments réjouissants. Enfin, la politique d'information en cas de transmission erronée de données témoigne de l'importance accordée aux impératifs de la protection des données (cf. ch. 3.11.2).

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 24,65 millions de francs, alors que 116,5 millions de francs devaient être consacrés à l'exploitation (montants budgétés). Quant au coût total du Bureau, il s'est maintenu à quelque 0,25 million de francs. Même si des audits contribuant à renforcer la protection des données (cf. ch. 3.3.2) ont à nouveau eu lieu et que les activités du groupe spécialisé dans la sécurité (cf. ch. 3.3.1) méritent une mention positive, il n'en reste pas moins que le rapport entre les montants consacrés à l'informatique d'une part et à la protection des données d'autre part reste insatisfaisant.

3.2.4 Tâches

La nouvelle loi sur les communes ne prévoit plus l'approbation des règlements sur la protection des données, ce qui a déchargé le Bureau de diverses formalités. Par contre, le volume de travail occasionné par l'examen préalable des règlements n'a pas diminué.
Lors de l'élaboration de l'ordonnance portant introduction de la loi fédérale sur le recensement de la population, il a été établi que les commissions communales de surveillance pour la protection des données assumeraient la fonction d'autorité de surveillance au sens de la législation fédérale. Quant au Bureau, il n'exercera que la haute surveillance (contrairement à ce qui s'était passé lors du recensement de 1990, auquel les commissions communales n'avaient guère participé). En tout état de cause, le Bureau ne pourra fournir qu'un minimum de prestations (instructions avant tout) dans ce domaine, au détriment de ses tâches ordinaires. S'il apparaît justifié de faire davantage appel aux commissions communales de surveillance (autonomie communale, proximité par rapport aux services chargés du recensement), on ne saurait ignorer qu'une fois de plus, des autorités de milice – d'une manière générale insuffisamment formées à leurs tâches en matière de protection des données – sont appelées à assumer des responsabilités sans avoir reçu des instructions suffisantes sur la manière de résoudre certaines questions particulières.

3.2.5 Registres

Faute de ressources, le registre ne contient aucune donnée supplémentaire par rapport aux années précédentes. Il en résulte que le mandat légal de base (saisie de tous les fichiers) n'est toujours pas rempli, et que les informations relatives aux 812 fichiers enregistrés n'ont été ni contrôlées sous l'angle juridique, ni mises à jour. Certains services administratifs ont annoncé l'existence de nouveaux fichiers. De telles communications n'ont fait l'objet ni d'un examen juridique, ni d'une saisie dans le registre informatisé.

3.3 Sécurité des données

3.3.1 Consignes

Le groupe spécialisé dans la sécurité instauré par la Conférence informatique cantonale a proposé à cette dernière de reprendre la réglementation zurichoise sur le classement des applications informatiques. L'Office d'organisation a ensuite été chargé d'examiner si cette réglementation, qui se fonde sur un manuel de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (IT-Grundschutzhandbuch), est transposable et compatible avec l'organisation informatique du canton de Berne. Pour sa part, le Bureau salue la décision prise par la Conférence informatique cantonale.

3.3.2 Audits: contrôles de la sécurité

L'Office d'organisation a confié à une entreprise externe le mandat d'examiner la sécurité de l'infrastructure du serveur web cantonal. Alors qu'un premier examen n'avait pas décelé de problème, un second examen (piratage éthique) a révélé des lacunes, et notamment l'existence d'une fuite imputable à une société chargée du suivi d'une page web. Depuis lors, il a été remédié aux lacunes constatées. Cette démarche a renforcé la conviction selon laquelle les audits peuvent contribuer à accroître sensiblement la sécurité, et il convient de relever le grand engagement dont l'Office d'organisation fait preuve à cet égard.

3.3.3 Sécurité du courrier électronique

Le Conseil-exécutif a approuvé en date du 10 novembre 1999 la clôture du projet BEMAIL dont l'un des objectifs était de garantir la sécurité des couriels échangés, à l'intérieur de l'administration, entre les services tenus à la prudence de par la nature des données qu'ils traitent. Or, cet objectif n'a pas pu être atteint. Des solutions techniques ont certes été trouvées pour de petits groupes d'utilisateurs, et il semble en particulier que le service de certification s'est bien acquitté de sa tâche (infrastructure à clé publique). Toutefois, la diffusion n'a pas pris les proportions souhaitées, notamment en raison de l'influence exercée par l'évolution rapide du contexte général: s'il s'est avant tout agi, dans un premier temps, de garantir la confidentialité des couriels à l'intérieur de l'administration, un besoin de validité et d'authenticité s'est rapidement fait sentir, surtout pour les échanges avec des interlocuteurs externes à l'administration. Le produit utilisé permettait la signature électronique au niveau interne, mais les normes faisaient défaut pour l'utilisation d'une clé privée. De plus, il était pratiquement impossible de respecter les consignes connues, comme celles qui valent en Allemagne, sans recourir à des cartes à puce. Les procédures censées offrir une solution de remplacement (clé sur disquette) ne respectaient pas les exigences (allemandes) en matière de sécurité, et n'étaient pas non plus acceptées par les utilisateurs. Il convient malgré tout de relever que les responsables du projet ont fait preuve d'un grand engagement en faveur des questions de sécurité.
Compte tenu de l'interdiction, toujours en vigueur, de transmettre par couriel des données particulièrement dignes de protection sans cryptage, l'exigence de sécurité en matière de courrier électronique conserve toute sa validité. Dans le cadre du projet BEMAIL II, il s'agira de permettre l'échange de messages portant une signature électronique dans un cercle élargi de partenaires.

3.4 Projets informatiques

Le projet Gelan 2002 de la Direction de l'économie publique, qui doit permettre la mise en œuvre des consignes fédérales sur le versement de contributions aux agriculteurs, prévoit désormais le traitement des sanctions administratives. Comme il s'agit de données particulièrement dignes de protection, les exigences s'accroissent tant au niveau de la sécurité qu'en ce qui concerne les bases légales (procédure d'appel). Il est maintenant prévu d'exploiter le système en commun avec les cantons de Fribourg et de Soleure.
Le Bureau n'a pu se prononcer sur le projet de bracelet électronique de l'Office de la privation de liberté et des mesures d'encadrement (possibilité offerte aux personnes condamnées à une peine privative de liberté de courte durée de purger cette dernière à leur domicile en portant un émetteur à la cheville; phase de test de 1999 à 2003) qu'en reprenant le rapport de son homologue de Bâle-Campagne. Il a fallu exiger l'élaboration systématique d'une stratégie concernant la sécurité.
Il est renvoyé au chiffre 3.10 s'agissant du projet OBV 99 de la centrale des amendes d'ordre, et au chiffre 3.5 en ce qui concerne les projets GRIS (système d'information parlementaire sur Internet) et STEZE (communication par Internet avec la centrale des remplacements de la Direction de l'instruction publique).
Le projet BKM-2000 (logiciel de gestion des coûts de construction destiné à planifier, piloter et contrôler les investissements de travaux publics) a soulevé la question du caractère obligatoire ou facultatif de la prise de position du Bureau sur les projets informatiques qui est prévue dans le guide de l'Office d'organisation sur le déroulement de projets. En tout état de cause, ni la loi ni aucune ordonnance n'imposent une telle prise de position. Il est d'ailleurs fréquent que les organes compétents pour autoriser les dépenses approuvent des projets informatiques sans que le Bureau n'ait été

consulté. Cette pratique n'est certes en rien contraire à la loi, mais elle est regrettable au vu de l'importance capitale que revêtent les projets informatiques pour le Bureau. Force est toutefois de constater qu'un examen en temps opportun de tous les projets informatiques empiéterait considérablement sur le temps consacré aux autres domaines d'activité.

3.5 Internet

Consulté par la Direction de l'instruction publique (pages web des écoles) et par les responsables des projets STEZE et GRIS, le Bureau a relevé que la publication de données personnelles sur Internet équivaut à l'instauration d'une procédure d'appel à l'échelle mondiale et requiert de ce fait une base légale. Une ordonnance suffit dans le cas de données qui ne sont pas particulièrement dignes de protection, pour autant que les personnes concernées aient une possibilité de blocage inconditionnelle. Il est admissible, dans une phase transitoire, de s'en tenir à l'approbation expresse des personnes concernées capables de discernement. Cependant, les élèves de l'école obligatoire n'ont en règle générale pas cette capacité – sauf dans des cas simples – lorsqu'il s'agit d'Internet. Par ailleurs, une personne occupant une fonction publique n'a pas à tolérer que des services cantonaux publient son adresse privée ou sa photo sur Internet. Il a fallu insister une nouvelle fois sur le fait que les pages web doivent être protégées contre le piratage. Les formulaires diffusés sur Internet ne peuvent être utilisés que si l'identité des utilisateurs est vérifiable d'une autre manière ou sans importance. La diffamation d'un enseignant sur le livre d'or du site web d'une école a rappelé la responsabilité de l'éditeur d'un site quant au contenu de ce dernier. Si la commune responsable interdit la communication de listes du contrôle des habitants, l'école ne saurait rendre cette interdiction vaine par son site Internet. Le canton et les communes ont très rapidement adopté Internet comme instrument de travail, et il importe maintenant que l'élaboration des bases légales nécessaires suive le même rythme.

3.6 Législation

Le projet de nouvelle loi sur la santé publique prévoit que patient et médecin peuvent convenir que le dossier sera délivré au patient, au lieu d'être conservé pendant 20 ans par le médecin. Cette disposition tient compte d'une ancienne revendication en matière de protection des données.
La Direction de l'économie publique a élaboré un projet d'ordonnance sur la vente de données. Fondée sur la législation relative à l'information du public (principe de la publicité), cette ordonnance exploratoire aurait dû permettre la vente de données pendant une période limitée. Les travaux préparatoires, caractérisés par une grande transparence et l'écoute des voix critiques, ont permis d'aboutir à la conclusion que la vente de données par le canton est une prestation qui n'est susceptible d'être offerte que si l'égalité de traitement est garantie au plan juridique; de plus, l'atteinte qu'elle porte au droit fondamental à la protection des données est suffisamment grave pour requérir une base légale au sens formel (il n'y a pas lieu d'évoquer ici les particularités de l'ordonnance exploratoire dont la validité est limitée dans le temps), mais cette atteinte est amoindrie par l'existence d'un droit de blocage inconditionnel pour autant que la possibilité d'exercer ce droit soit garantie.
Le Bureau a d'emblée pu prendre part aux travaux préparatoires. La Direction de l'économie publique a décidé de ne pas poursuivre le projet plus avant compte tenu des résultats de la procédure de corapport.
L'ordonnance portant introduction de la loi fédérale sur le recensement fédéral de la population permet aux communes de compléter leur registre des habitants en indiquant pour chaque personne le numéro de ménage ou de logement attribué par le registre fédéral des bâtiments et des logements. Les données et les liens établis entre elles ne peuvent être utilisés qu'à des fins statistiques. La nécessité d'une telle base légale est indéniable dans la perspective du recensement de 2010. Quant à l'assurance que la composition des ménages n'est pas enregistrée à d'autres fins, elle dépend des moyens techniques et organisationnels mis en œuvre pour combattre les abus (cf. également ch. 3.2.4).
Le groupe de travail des organes de protection des données des cantons et de la Confédération a examiné le projet de loi fédérale sur les documents d'identité des ressortissants suisses. Le délégué à la protection des données du canton de Zurich a élaboré une prise de position sur ce projet, et une autre sur l'avant-projet de modification du Code civil suisse concernant la tenue informatisée des registres de l'état civil, que le Bureau a intégralement reprises. Chacun des deux projets prévoit un registre central à l'échelle suisse avec un accès en ligne pour la police. L'ordonnance de 1994 relative à la carte d'identité suisse ne prévoyait quant à elle d'accès en ligne à la banque de données qu'à des fins administratives. Il convient à cet égard de rappeler le rapport de la Commission de gestion du Conseil des Etats daté de novembre 1998, selon lequel la mise en place d'un accès en ligne de la police doit être précédée d'un examen transparent de sa nécessité et de sa conformité aux principes de proportionnalité et de finalité. Cet impératif doit être souligné du point de vue cantonal.

3.7 Collectivités de droit communal

Comme par le passé, une grande partie des avis juridiques – donnés pour la plupart par téléphone – étaient destinés aux collectivités de droit communal. Ces dernières sont elles aussi en train d'examiner les conditions de la création de sites sur le web. Dans ce contexte, il a notamment fallu préciser que l'annonce des départs au contrôle des habitants par le biais d'un formulaire de communication en ligne ne respectait pas les consignes de sécurité.
Le règlement type sur la protection des données a été adapté aux nouvelles dispositions légales (suppression de l'approbation cantonale, base légale cantonale pour l'accès en ligne de la Police cantonale aux données du contrôle des habitants). (S'agissant du recensement, cf. ch. 3.2.4 et 3.6.)

3.8 Archives

L'entrée en vigueur de la législation sur l'information du public a soulevé la question de savoir à quel moment un tiers peut consulter des données archivées particulièrement dignes de protection. Concrètement, une demande visant la consultation d'arrêtés du Conseil-exécutif remontant à plusieurs années est à l'origine de l'examen de la question. D'entente avec le Service juridique de la Chancellerie d'Etat, il a été précisé qu'aussi longtemps qu'une personne est en vie, il n'existe pas de droit de consulter les données particulièrement dignes de protection qui la concernent. Après le décès de la personne, il convient d'appliquer par analogie, sous réserve du respect de la mémoire, la loi fédérale sur l'archivage selon laquelle les archives peuvent être consultées librement après l'expiration d'un délai de protection de 30 ans qui court à partir de la date du dernier document, pour autant que la personne soit décédée depuis au moins trois ans. Si la date du décès n'est pas connue, on admet que la personne n'a pas dépassé l'âge de 110 ans. En tout état de cause, il n'est guère satisfaisant que les auto-

rités chargées de l'application du droit comblent elles-mêmes de telles lacunes juridiques, et l'édiction d'une loi cantonale sur l'archivage semblerait judicieuse.

3.9 Recours à l'informatique dans les hôpitaux

3.9.1 Réglementation de l'accès à un système d'information hospitalier

La Direction de la santé publique et de la prévoyance sociale a indiqué dans une décision sur recours qu'un patient avait droit à ce que les données administratives le concernant soient effacées d'un système autorisant leur consultation par tous les services de l'hôpital. En effet, la configuration d'un tel système est disproportionnée et la simple mention d'un traitement antérieur dans un autre service peut porter atteinte au droit fondamental du patient à la protection de ses données. De telles considérations auraient dû conduire au remplacement du système, qui était de toute manière prévu pour d'autres raisons.

3.9.2 Externalisation

L'Hôpital de l'Ile a externalisé le domaine de l'informatique, qu'il a confié au Zentrum für Informatik im Gesundheitswesen dont le siège est à Langenthal, fondé avec la société Atag debis Informatik AG. L'entreprise a repris 25 collaborateurs et deux apprentis. Dans le message de mars 1988 concernant la loi fédérale sur la protection des données, il est encore précisé que les données soumises au secret médical ne peuvent être traitées par des tiers qu'avec l'accord du patient. Interrogé par le groupe de travail des organes cantonaux de protection des données, l'Office fédéral de la justice a indiqué qu'il considère désormais la situation différemment: selon lui, les tiers traitant des données – par exemple les centres de prestations informatiques – sont des auxiliaires au sens de la réglementation relative au secret professionnel, de sorte qu'ils sont eux aussi tenus au secret médical. Ainsi, l'externalisation est possible même sans l'assentiment du patient, à condition que le principe de la proportionnalité soit respecté. Il appartient donc à l'hôpital mandant de veiller à ce que la société d'informatique n'utilise pas les données qu'elle traite à des fins internes, par exemple pour le recrutement du personnel. L'Office fédéral de la justice ajoute qu'à l'heure actuelle déjà, les médecins et leurs auxiliaires doivent tenir compte des diverses réglementations sur l'obligation de témoigner contenues dans les codes de procédure cantonaux et que l'externalisation du traitement des données dans d'autres cantons n'aggrave pas ce problème, seule une uniformisation de la procédure pénale à l'échelle suisse étant susceptible d'apporter une solution à cet égard. L'office fédéral estime en outre que dans certaines circonstances, il est permis au centre informatique de demander à être délié du secret médical indépendamment de l'hôpital qui lui a confié le traitement de ses données. Il ne devrait toutefois guère être admis de délier un centre du secret pour tout un groupe de personnes, par exemple dans le cadre de recherches par recoupements, car la pesée des intérêts qui est prescrite à cet égard devrait avoir lieu pour chaque cas individuellement. Enfin, l'office fédéral a précisé qu'il appartient au législateur cantonal de décider s'il entend, dans sa législation sur la santé publique, interdire l'externalisation à l'étranger.
L'Office fédéral de la justice constate à juste titre que la tendance à confier le traitement des données médicales à des entreprises externes s'est sensiblement accrue ces dernières années. Bien qu'un jugement pénal sur l'extension du champ d'application de la norme pénale fasse encore défaut, il ressort de l'avis exprimé par l'Office fédéral de la justice que l'externalisation du traitement des données par un hôpital n'est plus contraire au droit, mais que cette possibilité ne peut être exploitée qu'à condition d'accorder un soin tout particulier au choix et à la surveillance de l'entreprise mandatée et de lui donner des instructions précises. Cette condition requiert en particulier du mandant l'examen attentif des normes juridiques que doit appliquer son partenaire ainsi que la formulation de consignes très strictes, dans un contrat, sur le traitement des données et les contrôles. Il apparaît opportun que le législateur intervienne à cet égard; en effet, ce n'est qu'en présence de normes définies au terme d'une procédure législative détaillée qu'il sera possible d'admettre que le changement de point de vue n'a pas été avant tout dicté par les circonstances. En tout état de cause, il importe de surveiller l'évolution, qui va indéniablement vers une plus grande ouverture.

3.10 Points abordés dans le rapport précédent

3.10.1 Centrale des amendes d'ordre

Le système informatique choisi par la centrale des amendes d'ordre conduisait, pour des motifs comptables, à un enregistrement illicite des débiteurs d'amendes. En 1997 encore, la Direction de la police et des affaires militaires a renoncé pour des raisons financières à l'adaptation du programme. Toutefois, le système a dû être remplacé dans la perspective du passage à l'an 2000, et le nouveau système (OBV 99) tient compte des exigences formulées naguère.

3.10.2 Autorisation d'exploitation pour les systèmes de traitement des données de la Police cantonale

Les travaux préparatoires en vue d'un arrêté du Conseil-exécutif sont toujours en cours.

3.11 Cas particuliers

3.11.1 ADN

En 1999, le Grand Conseil a traité trois motions, une interpellation et une question concernant l'ADN, ce qui témoigne bien de l'importance capitale que revêt ce sujet. Le canton de Berne a également pris position sur le projet de loi fédérale sur l'analyse génétique humaine à l'occasion de la procédure de consultation. Le Bureau a pris connaissance du rapport établi par le groupe de travail fédéral sur la création d'une banque nationale de données de profils ADN. Le projet de loi cantonale sur l'exécution des peines et mesures envoyé en consultation contient une modification indirecte du Code de procédure pénale créant la base légale d'une banque de données ADN ainsi que de l'utilisation du matériel génétique, des produits dérivés et des données analysées à des fins d'identification judiciaire. Enfin, la Direction de l'instruction publique a élaboré un projet de directives sur la protection de la personnalité et des données à l'Institut de médecine légale. Les analyses d'ADN sont donc devenues un thème récurrent pour le Bureau, qui a par exemple dû répondre à la question de savoir quels sont les moyens, sur la base des données de l'état civil notamment, de déterminer si quelqu'un est bien, comme on le suppose, le père biologique d'une personne; cette question lui a été soumise après que l'analyse de l'ADN du père social déjà âgé d'une personne de plus de 40 ans effectuée sur mandat de cette dernière avec le consentement de l'intéressé avait confirmé que le père social ne pouvait pas être le père biologique.
Si le débat relatif aux données ADN a d'abord porté sur des aspects ponctuels (Une prise de sang en vue d'une analyse de l'ADN est-

elle admissible dans le cadre d'une poursuite pénale? La police peut-elle gérer une banque de données ADN?), il s'est de plus en plus généralisé, notamment sous l'influence du projet de loi fédérale sur l'analyse génétique humaine. Cette tendance est attestée aussi bien par le traitement des interventions parlementaires que par les prises de position concernant le projet de modification du Code de procédure pénale. La nouvelle dimension juridique du traitement des questions liées à l'ADN imposée par l'article 24novies de la Constitution fédérale (désormais art. 119, 2e al., litt. f) devrait être prise au sérieux: le patrimoine génétique d'une personne ne peut être analysé, enregistré et communiqué que si les conditions applicables ont été discutées et définies dans le cadre d'une procédure législative démocratique (cf. également le 6e rapport d'activités du préposé fédéral à la protection des données, pp. 283 à 285).

3.11.2 Réduction des primes d'assurance-maladie, interversion de deux supports de données

Le canton adresse aux assureurs des données leur permettant de diminuer directement le montant des factures de primes des personnes ayant droit à une réduction. A l'occasion d'un tel transfert de données, deux bandes magnétiques ont été interverties. Les assureurs ont signalé l'erreur et restitué les bandes. Le directeur de la justice, des affaires communales et des affaires ecclésiastiques a ordonné une analyse des procédures administratives internes. Cet incident témoigne bien des risques inhérents à l'utilisation de l'informatique. Cependant, la réaction des responsables – et en particulier l'information du public au sujet de cette affaire – montre également que ces risques sont pris au sérieux.

11 janvier 2000

Le délégué à la protection des données: *Siegenthaler*