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): **- (1998)**

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

PDF erstellt am: **16.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-544958

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

3.1 Introduction

3.1.1 1998 en bref

Deux services administratifs ont confié à une entreprise externe spécialisée l'examen de leur système informatique sous l'angle de la sécurité. L'entreprise étant dans les deux cas parvenue à pénétrer dans ledit système (piratage simulé), les services ont en fin de compte considérablement amélioré la sécurité de leurs applications.
La nouvelle loi sur la police soumet les systèmes de traitement des données de la Police cantonale à une autorisation d'exploitation du Conseil-exécutif. Le législateur a ainsi voulu introduire un contrôle renforcé. En conséquence, la police a dû reporter la création d'une banque de données ADN (patrimoine génétique) en raison de l'insuffisance des bases légales.

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

La conférence a demandé dans une résolution que les banques de données ADN ne soient mises sur pied qu'en fonction de bases légales claires et précises, que le stockage des analyses génétiques d'identification soit susceptible d'être contrôlé par le juge, que les empreintes génétiques soient immédiatement détruites en cas d'acquittement, que les échantillons d'identification ne puissent être réutilisés que dans des buts de poursuite pénale, que la durée de conservation soit assortie de délais d'examen et de destruction appropriés, et que les laboratoires responsables soient soumis à des exigences qualitatives strictes. La conférence estime par ailleurs que de telles exigences ne doivent pas être limitées à l'utilisation des codes génétiques, mais s'étendre à celle de tout matériau cellulaire humain. La résolution demande en outre que la conservation de matériau génétique humain – qu'une base légale claire doit prévoir – soit confiée à un tiers indépendant (cf. également ch. 3.8.2).
Sans autorisation expresse contenue dans le droit fédéral ou cantonal, aucune donnée personnelle ne doit pouvoir être consultée au moyen d'une procédure d'appel, comme l'a indiqué le préposé fédéral à la protection des données dans sa réponse (publiée) à la question de l'admissibilité d'un accès en ligne de l'Intendance des impôts à la banque de données de l'Office de l'agriculture.

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. Conforme aux attentes de la clientèle, cette solution fait toutefois apparaître d'autant plus préjudiciables les longs délais – souvent de plus d'une année – applicables au traitement des autres affaires. Les ressources disponibles restent insuffisantes pour permettre au Bureau d'accomplir son mandat légal; c'est ainsi qu'il n'est notamment pas possible de procéder à des inspections, dont l'importance n'est toutefois pas mise en doute par le Bureau, pas plus que par les services qui traitent des données.

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. Des cours de formation et de perfectionnement ont eu lieu à la fréquence usuelle. Il reste vrai que l'attitude des cadres par rapport aux questions de protection des données varie fortement d'une personne à l'autre. L'Office d'organisation et la Direction de la justice, des affaires communales et des affaires ecclésiastiques ont témoigné d'un sens aigu de leurs responsabilités en commandant de leur propre initiative un audit en matière de sécurité (cf. ch. 3.1.1 et 3.3.2). Les audits ont été financés au moyen de ressources propres aux Directions. Le fait que la Direction de la justice, des affaires communales et des affaires ecclésiastiques justement ait opté pour une telle démarche mérite d'être relevé: le comité de contrôle de la sécurité informatique qu'elle a mis en place conçoit sa tâche comme un processus continu. En lui emboîtant le pas, les autres Directions renforceraient leur responsabilité propre. D'ailleurs, la mise en place, par la Conférence informatique cantonale, du groupe de travail «security» va dans le même sens: sa tâche est de résoudre les questions liées à la sécurité qui concernent plusieurs Directions à la fois.

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 25,9 millions de francs en 1998, alors que 120,4 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. Les deux audits financés par les Directions ont directement contribué à renforcer la sécurité des données, et le déblocage de quelques dizaines de milliers de francs pour des mesures de contrôle est réjouissant. Il n'en reste pas moins que les contrôles effectués (cf. ch. 3.3.2) ont avant tout montré à quel point il est nécessaire de modifier le rapport entre les montants consacrés à l'informatique d'une part, et à la protection des données d'autre part.

3.2.4 Nouvelles tâches

Le Conseil-exécutif a désigné le Bureau comme étant l'organe de contrôle du respect de la protection des données lors du recensement 2000. Or, le projet d'ordonnance concernant ce recense-

ment confère un vaste cahier des charges à l'organe de contrôle, et sans ressources supplémentaires, il ne sera pas possible de le respecter. Lors du dernier recensement, le même problème avait déjà abouti à ce que la Commission de gestion soit saisie en sa qualité d'autorité de surveillance.

3.2.5 Registre

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 (cf. également le ch. 3.8.1 sur la question du bien-fondé de la tenue du registre).

3.3 Sécurité des données

3.3.1 Consignes du Conseil-exécutif

Par manque de temps, l'exactitude des classifications des applications informatiques fournies par les Directions sur la base de l'arrêté du Conseil-exécutif 4637/92 n'a toujours pas pu être examinée (cf. toutefois ch. 3.8.1), pas plus que la mise en œuvre des mesures prévues.
L'ordonnance du Conseil-exécutif sur l'établissement et le séjour des Suisses prévoit que la directive S02 de l'Office fédéral de l'informatique s'applique par analogie à l'accès en ligne de la Police cantonale aux données du contrôle des habitants. Une telle consigne en matière de sécurité des données devrait avoir valeur d'exemple pour toutes les applications informatiques.
Dans ses directives révisées régissant l'utilisation de mots de passe, le Conseil-exécutif a fixé la longueur minimale des mots de passe à six signes (contre cinq auparavant). Les directives, détaillées, s'adressent non seulement aux utilisateurs et utilisatrices, mais aussi aux responsables des systèmes et des applications. Les audits ont révélé que même dans leur version remaniée, elles ne satisfont pas pleinement aux exigences de sécurité (cf. également ch. 3.3.2). Une nouvelle adaptation des directives aurait certes été envisageable, mais une mise en œuvre à court terme ne semblait guère possible, notamment du fait que la teneur actuelle a été reprise dans le programme de formation Save achevé en 1998. Le problème a toutefois été reconnu et l'Office d'organisation s'emploie à le résoudre.

3.3.2 Audits: contrôles de la sécurité

La loi sur la protection des données permet de donner mandat à des tiers de traiter des données. Cette base légale autorise aussi les contrôles de sécurité (piratages simulés) effectués par des tiers, à condition que le soin nécessaire soit apporté à leur choix, à leur instruction et à leur surveillance. Il s'agit par ailleurs de minimiser les risques d'abus grâce aux possibilités offertes par le droit. De plus, les autres services cantonaux concernés doivent être pris en considération. C'est ainsi que la Cour suprême a été informée de la démarche entreprise par la Direction de la justice, des affaires communales et des affaires ecclésiastiques. Pour des raisons de sécurité, les modalités de contrôle choisies ne sauraient être exposées de manière précise dans le présent rapport, vu le caractère public de ce dernier. Il s'agira toutefois de fournir des informations détaillées à la Commission de gestion du Grand Conseil. En bref, le contrôle a consisté à examiner s'il existait des possibilités d'accès aux données, et de telles possibilités ont été décelées. Le résultat du contrôle se résume comme suit: l'intégration dans Internet, l'équipement technique et la qualité des installations, de même que la vigilance des responsables du réseau ont été notés positivement. L'ordinateur coupe-feu a empêché toute intrusion, et les responsables ont non seulement immédiatement remarqué la tentative, mais ont également réagi promptement. L'examen a par ailleurs révélé que des améliorations étaient susceptibles d'être apportées aux limitations tant physiques qu'organisationnelles de l'accès et à la qualité des mots de passe ainsi que de certaines autres configurations. Bon nombre des lacunes constatées ont pu être en grande partie comblées par une réorganisation et une reconfiguration, et les contrôles internes des mots de passe, qui ont été jugés nécessaires, ont débuté depuis lors. Les mandants ont pris les résultats de l'audit très au sérieux. Ils ont aussi rapidement réalisé les mesures proposées, du moins lorsqu'elles n'engendraient pas – et c'était le cas de la plupart d'entre elles – des dépenses importantes (extensions, remplacement). Au niveau interne, les lacunes constatées ont été exposées clairement et sans ménagement. Les responsables ont été de toute évidence fortement sensibilisés aux problèmes. Le point de vue du Bureau est mitigé: d'une part, il est très probable que la situation n'est pas meilleure dans les services cantonaux qui n'ont pas fait l'objet d'un contrôle, et d'autre part, les mêmes vérifications effectuées dans l'économie privée aboutissent à des résultats semblables. Il convient d'en déduire que la sécurité informatique ne dépend pas de la configuration, une fois pour toutes, du système choisi, mais ne peut résulter que de contrôles répétés, semblables à ceux dont il a été question ici (cf. ch. 3.2.2).

3.3.3 Virus

Les virus continuent à menacer gravement la sécurité informatique. En 1998, le Bureau a été confronté pour la première fois à des virus imaginaires (hoaxes), qui représentent un problème en raison de la charge de travail (inutile) qu'ils engendrent.

3.4 Législation

Les bases légales de procédures d'appel ont été créées dans plusieurs ordonnances; c'est ainsi notamment que l'ordonnance sur l'établissement et le séjour des Suisses prévoit une procédure d'appel par laquelle la Police cantonale peut consulter les données du contrôle des habitants. La nouvelle loi sur les impôts devant entrer en vigueur en 2001 pose également une base pour de telles procédures, et prévoit la possibilité de déclarations d'impôt informatisées. Quant à la publicité du registre d'impôts, elle ne subit aucun changement. Par ailleurs, l'ordonnance sur les exceptions à l'obligation de détruire les données de la police a été édictée en réponse au mandat contenu dans le Code de procédure pénale de réglementer cette matière. Elle autorise la conservation au-delà des délais légaux des données concernant en particulier les victimes, les personnes disparues ou les personnes dangereuses ainsi que des données concernant les crimes imprescriptibles. Enfin, l'ordonnance sur la recherche oblige la Commission d'éthique à informer le chercheur ou la chercheuse des autorisations supplémentaires requises lors de la procédure d'autorisation. Il s'agit avant tout d'autorisations de la Commission fédérale d'experts du secret professionnel en matière de recherche médicale.

3.5 Internet, sécurité du courrier électronique, téléphonie

3.5.1 Internet

A ce jour, plusieurs Directions ont édicté des directives concernant l'utilisation d'Internet par leur personnel. Le Bureau a quant à lui établi un document type sur la base des directives de la Chancellerie d'Etat. En cas d'abus – et il y en a, comme il fallait s'y attendre – les directives permettent un contrôle tout en respectant la sphère privée des collaborateurs et collaboratrices.
En l'espace d'une année, Internet est devenu un auxiliaire de travail quotidien au sein de l'administration cantonale. Les agents et agentes se procurent des informations par ce biais, et le canton s'en sert pour ses relations publiques et ses communications internes. Les pages Web du canton envoient elles aussi des témoins (ou cookies: informations enregistrées sur le disque dur de la personne qui visite un site, en règle générale inoffensives, mais susceptibles d'être utilisées pour évaluer le comportement de l'internaute) ou invitent à contacter des services administratifs par courrier électronique, sans pour autant attirer l'attention sur les risques inhérents à ce type d'opérations. Les témoins ne doivent pas servir à surveiller les personnes qui visitent les sites de services cantonaux, comme le précisait déjà le rapport de l'année précédente. Si les témoins sont malgré tout maintenus, il convient au moins d'en expliquer la signification concrète aux internautes, et toute invitation à envoyer un message électronique devrait préciser que ce dernier offre une sécurité à peu près identique à celle d'une carte postale.

3.5.2 Sécurité du courrier électronique

Une partie des messages électroniques échangés à l'intérieur de l'administration continue à transiter par un centre de calcul de Warwick (GB). Le cryptage des messages au niveau interne prévu dans le cadre du projet BEMAIL se trouve en phase pilote, de sorte que les postes de travail sûrs à cet égard sont encore peu nombreux. L'élaboration, d'ici en 2000, d'une réglementation concernant la signature numérique par l'Office fédéral de la communication augmente les chances de disposer de liaisons électroniques sûres dans un proche avenir.

3.5.3 Recherche avec Internet et sur Internet

L'Institut de sociologie de l'Université de Berne a enquêté sur les habitudes des internautes par le biais d'un questionnaire électronique, avec la collaboration d'un grand fournisseur d'accès, et a examiné les comportements de participants à des forums de bavardage. Dans les deux cas, les consignes relatives à la protection des données applicables aux projets de recherche n'ont pas été respectées. S'agissant du premier projet, la sécurité de la transmission électronique des réponses n'a pas été examinée, et aucune mesure n'a été prise au plan juridique pour garantir que le fournisseur d'accès ne transmette les réponses reçues qu'à l'Institut de sociologie. En cas d'abus, le canton aurait par exemple dû assumer des frais de l'ordre de quelques centaines de francs par personne ayant répondu pour le changement de son adresse Internet. Les dommages n'auraient certes pas été d'une extrême gravité, mais le nombre des personnes ayant pris part à l'enquête se monte tout de même à 17000. A cela s'ajoute que les questionnaires contenaient des données particulièrement dignes de protection. Dans le cas du second projet, il a fallu relever qu'il est interdit de noter la fréquence à laquelle des participants à des forums de bavardage non anonymes se connectent à Internet sans l'autorisation de ces derniers.

3.5.4 Frais de téléphone

Dans une prise de position destinée à la Commission de gestion du Grand Conseil, le Bureau a indiqué en substance que les bases légales actuelles ne permettent ni au supérieur ou à la supérieure hiérarchique, ni au Contrôle des finances, d'évaluer à des fins de contrôle l'intégralité des données téléphoniques (numéro de l'appelant, numéro de l'appelé, moment de l'appel, durée, coût).

3.6 Collectivités de droit communal

Après la parution, dans le «Beobachter», d'un article consacré au traitement abusif de données par les communes, le nombre de demandes adressées au Bureau par des autorités communales a augmenté – bien que l'article n'ait pas mentionné de commune bernoise. Souvent, les questions posées par les responsables communaux ont attesté d'une bonne prise de conscience des impératifs de la protection des données. C'est ainsi que le Bureau a notamment répondu à des questions relatives à l'admissibilité de la transmission de données concernant des requérants d'asile et d'une photo de carte d'identité à des fins de recherche publique. Dans le premier cas, il convenait de restreindre la portée de la transmission de données, et dans le second, la condition était que la mesure ait été ordonnée par le juge d'instruction conformément au Code de procédure pénale. Deux commissions communales de surveillance pour la protection des données – simultanément commissions de vérification des comptes – ont indiqué au Bureau qu'à l'occasion de la révision des comptes, elles avaient constaté l'insuffisance des mesures de sécurité concernant tous les auxiliaires informatiques de la commune. La proposition a été émise que des services cantonaux apportent leur soutien en offrant des possibilités de formation et en établissant des listes de contrôle utilisables par des autorités de milice.
En matière de téléphonie, les communes se préoccupent des mêmes questions que le canton.
La communauté d'intérêt formée par les communes révèle notamment que ces dernières sont conscientes du problème soulevé par le passage à l'an 2000.

3.7 Points abordés dans le rapport précédent

3.7.1 Communication de données par les hôpitaux aux assureurs

Les services fédéraux poursuivent leurs travaux en vue de déterminer quelles données les hôpitaux doivent fournir aux assureurs en vue du décompte. La recommandation émise le 5 décembre 1997 par le Bureau de renoncer jusqu'à nouvel avis à la communication des codes de diagnostic CIM-10 reste donc valable.

3.8 Cas particuliers

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

La loi sur la police oblige la Police cantonale à requérir auprès du Conseil-exécutif une autorisation d'exploiter ses systèmes de traitement des données dont elle fixe le contenu de manière détaillée. Comme il fallait s'y attendre, la Police cantonale et le Bureau ont des avis divergents sur la mise en œuvre de cette

prescription, et ce dernier a rédigé une prise de position de 18 pages à cet égard. Il convient d'attendre l'arrêté du Conseil-exécutif pour rendre compte des détails de la procédure d'autorisation. En tout état de cause, la surveillance de la police en matière de protection des données pose problème à l'heure actuelle, comme en témoigne la nécessité de compléter et de corriger la classification des applications informatiques du Commandement de police prévue par l'arrêté du Conseil-exécutif 4637/92 (classification portant sur la confidentialité et la disponibilité). De plus, le caractère exhaustif de l'autorisation devrait être contrôlé sur la base du registre des fichiers, mais un tel examen est impossible étant donné que la Police cantonale n'a pas encore respecté l'obligation qui lui est faite depuis dix ans d'annoncer ses fichiers. Des documents de travail internes à la police et destinés à l'élaboration du registre ont certes été mis à la disposition du Bureau, mais ils ne permettent pas l'examen requis.
C'est à juste titre que l'on s'interroge aujourd'hui sur l'utilité d'un registre des fichiers, qui plus est centralisé. Il n'en reste pas moins que la plupart des autres services administratifs se sont acquittés de leur obligation, assumant la charge de travail considérable qui lui était liée, alors que la Police cantonale n'a toujours pas appliqué un arrêté du Conseil-exécutif pourtant motivé en particulier par la volonté de recenser ses propres fichiers.

3.8.2 **Banque de données ADN**

Dans sa prise de position du 14 décembre 1998, l'Office juridique de la Direction de la justice, des affaires communales et des affaires ecclésiastiques a recommandé à la Direction de la police et des affaires militaires de régler expressément l'utilisation d'une banque de données ADN dans une base légale formelle. Les travaux préparatoires en vue d'une autorisation d'exploitation pour les systèmes de traitement des données de la Police cantonale (cf. ch. 3.8.1 et 3.1.1) ainsi que de la résolution de la Conférence suisse des commissaires à la protection des données (cf. ch. 3.1.2) ont permis l'élaboration d'un avant-projet disponible au niveau interne fin août 1998 déjà. Les projets publiés de loi allemande concernant la constatation de l'identité au moyen de l'ADN, loi qui est entrée en vigueur depuis lors, ont également été d'une grande utilité.

Le 15 janvier 1999

Le délégué à la protection des données: *Siegenthaler*