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 2001 en bref

Le Bureau n'est plus appelé que dans de rares cas à participer à des projets informatiques. Cependant, plus la prise en compte des exigences de la protection des données intervient tard, plus les coûts en sont élevés, la progression étant à cet égard exponentielle. Il y a donc lieu d'institutionnaliser de toute urgence une intervention au stade initial des projets, comme l'ont confirmé des enquêtes effectuées au moment de l'octroi de crédits.
Les tunnels autoroutiers, les trains, les parkings couverts, les écoles et même, de manière générale, les places publiques commencent à faire l'objet d'une surveillance par caméras vidéo. Or, seule la création des bases légales nécessaires provoquera un débat politique sur le bien-fondé d'une telle utilisation des techniques actuelles. Dans ce contexte, il conviendra également de tenir compte du développement rapide des techniques de vidéosurveillance (p. ex. détection des événements).

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

L'association des Commissaires suisses à la protection des données (DSB+CPD.CH) a élaboré, avec le concours du préposé fédéral à la protection des données, une notice à l'attention des assureurs concernant les lettres de sortie et les rapports opératoires ainsi qu'une brochure sur les consignes en matière de sécurité informatique à l'intention des personnes travaillant dans l'administration. L'association a en outre rédigé une prise de position au sujet de six lois fédérales, et en a mis un projet à la disposition de ses membres dans la perspective de la consultation au niveau cantonal (cf. ch. 3.6). Elle a également examiné d'autres actes législatifs et constaté qu'ils tenaient suffisamment compte des impératifs de la protection des données, de sorte que les cantons membres n'ont pas eu besoin d'approfondir la question. L'association a également été représentée dans le groupe de travail mis sur pied par le Département fédéral de justice et police en vue de la révision partielle de la loi fédérale sur la protection des données, et entendue au sujet de la loi sur la transparence. Enfin, elle a organisé des cours de perfectionnement sur le thème «Internet et l'école» de même que – à l'occasion de la huitième Conférence suisse des commissaires à la protection des données – sur le traitement des projets informatiques (cf. ch. 3.4.2).

3.2 Description de tâches, priorités, moyens à dispositions

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. Le problème de la longueur des délais d'attente pour les avis de droit évoqué dans les rapports annuels précédents n'a toujours pas trouvé de solution (cf. ch. 3.2.2).

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

Sous le chiffre 10.2 de son rapport du 14 août 2001 sur le rapport de gestion 2000, la Commission de gestion du Grand Conseil a constaté des insuffisances chroniques dans l'accomplissement du mandat légal de la protection des données. Elle a donc recommandé au Conseil-exécutif de mettre à disposition les ressources humaines nécessaires pour remplir ce mandat légal (recommandation n° 6). Le gouvernement ne saurait toutefois envisager la création d'un poste suite à l'adoption par le Grand Conseil, en novembre 2001, d'une motion le contraignant à d'importantes mesures d'économie. Dans un premier temps, une amélioration doit donc être recherchée au moyen de transferts de tâches: les services compétents pour fournir des conseils dans leurs domaines spécialisés traiteront également des questions de protection des données; quant à l'examen des projets informatiques et aux activités de contrôle, ils devront faire l'objet de mandats à des tiers dont les coûts seront supportés par les services traitant des données (cf. ch. 3.2.5 et 3.4.2). Les travaux de mise en œuvre sont en cours.

3.2.3 Responsabilité propre des services traitant des données

Les cours de perfectionnement organisés par les services traitant des données (p. ex. le cours destiné à la Conférence informatique de la Direction des finances ou le cours offert par le délégué à la protection des données de l'hôpital de l'Ile en collaboration avec l'association datenschutzforum.ch) tout comme les nombreuses questions posées par les services administratifs attestent bien de l'engagement dont ces derniers font preuve dans le domaine de la protection des données. Les directives sur la protection des données au sein des trois cliniques psychiatriques cantonales, celles qui sont destinées aux centres de consultation pour les victimes d'infractions, de même que les directives sur l'utilisation des outils informatiques à la Direction des travaux publics, des transports et de l'énergie, toutes trois à l'état de projet, sont autant de contributions à la mise en œuvre des principes de la protection des données au quotidien. Une autre démarche positive mérite une mention: les contrôles effectués par l'Inspection de l'Intendance des impôts concernant les accès au système NESKO (procédure d'appel); ces accès aux données fiscales servent à l'examen, par l'Office des assurances sociales et de la surveillance des fondations, des demandes de réduction des primes d'assurance-maladie obligatoire.

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 20 millions de francs, alors que 129,6 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. Force est de constater que le rapport entre les montants consacrés à l'informatique d'une part et à la protection des données d'autre part reste insatisfaisant.

3.2.5 Contrôle du traitement de données informatiques

Dans l'autorisation d'exploiter les systèmes de traitement des données délivrée à la Police cantonale (cf. ch. 3.8.1) de même que dans le projet de nouvelle loi sur la BEDAG Informatik, le Conseil-exécutif prévoit l'obligation de faire périodiquement appel à des organes de contrôle indépendants. La diffusion du nouveau principe applicable aux contrôles évoqué dans le rapport précédent (obligation faite aux services traitant des données de recourir, à leurs frais, à des organes de contrôle indépendants) se poursuit.
C'est également en recourant à des spécialistes externes que le Contrôle des finances a procédé à une appréciation des risques liés à l'informatique auprès de toutes les Directions et de la Chancellerie d'Etat. L'examen, qui a porté sur le traitement de données tant personnelles que factuelles, a été d'une manière générale plus poussé que les examens prévus dans la loi sur la protection des données (p. ex. gestion des investissements dans les technologies de l'information). Il englobe en tout état de cause les objectifs de ces derniers puisque l'un des risques, dans ce domaine, est justement la violation de la protection des données. Faute de ressources suffisantes, le Contrôle des finances a toutefois renoncé à examiner la gestion des données. Ce choix souligne bien l'importance des ressources mobilisées par un tel examen, au vu de la situation privilégiée, à cet égard, du Contrôle des finances par rapport à celle du Bureau (2 postes à plein temps et des spécialistes externes). Les contacts établis avec le Contrôle des finances doivent permettre au Bureau de tirer parti des résultats de l'examen pour ses propres tâches.
Le chapitre 3.2.3 traite du contrôle effectué par l'Inspection de l'Intendance des impôts concernant les accès au système NESKO. D'une manière générale, les ressources dont dispose le Bureau ne lui permettent pas de procéder spontanément à des opérations de contrôle des systèmes informatiques.

3.3 Sécurité des données

L'Université de Berne a été victime d'une attaque de son système informatique semblable à celle qui a touché l'EPF de Zurich, bien que nettement moins grave (avalanche de courriels ou d'avis de non-remise). De tels incidents soulignent, s'il en est encore besoin, l'importance de la sécurité des données.

3.3.1 Consignes

Les consignes en matière de sécurité informatique dans l'administration cantonale, dont le caractère partiellement suranné, disparate et incomplet était déploré dans le rapport précédent, sont toujours en vigueur. Dans l'autorisation d'exploiter les systèmes de traitement des données qu'il a délivrée à la Police cantonale par exemple, le Conseil-exécutif précise que les systèmes en question doivent répondre aux exigences en matière de sécurité informatique qui sont applicables dans l'administration cantonale (cf. ch. 3.8.1). Ce renvoi – pleinement justifié – implique l'existence de consignes efficaces, également en cas d'externalisation de prestations informatiques. Pourtant, de telles consignes font toujours défaut.

3.3.2 Sécurité du courrier électronique

L'Office d'organisation a précisé au printemps que les essais en cours sur la sécurité du courrier électronique, qui utilisaient les certificats de Swisskey, se déroulaient à la satisfaction de tous les participants. Swisskey a toutefois révoqué l'ensemble de ses prestations au début de l'été. La Conférence informatique cantonale a donc décidé en novembre d'interrompre la phase pilote du projet portant sur la sécurité du courrier électronique, vu qu'aucun service de certification n'était plus en mesure de garantir à long terme des prestations satisfaisantes. Il a été conseillé aux entités particulièrement exposées, comme les cliniques psychiatriques et les services du personnel, de se rabattre sur les solutions disponibles pour leur domaine d'activité (p. ex. PGP).
La décision de la Conférence informatique cantonale est compréhensible. La cessation des activités de Swisskey représente un sérieux revers, d'autant plus que l'Office d'organisation avait constaté qu'un système de courrier électronique sûr pouvait dans la pratique se révéler convivial et ne requérir qu'une initialisation de moins de dix minutes par poste de travail. Ainsi, le grand engagement – couronné de succès – dont ont fait preuve l'Office d'organisation et l'Office du personnel dans la recherche de solutions techniques n'a pas été récompensé puisque la diffusion d'un système de messagerie électronique offrant toutes les garanties de sécurité a échoué faute de service de certification, et ce constat d'échec est particulièrement cuisant (cf. ch. 3.5 au sujet de l'envoi des déclarations d'impôt par courrier électronique, et ch. 3.6 s'agissant de la loi fédérale sur la signature électronique).

3.4 Projets informatiques

3.4.1 Projets en cours de réalisation

Les responsables des projets GRUDIS (système d'information sur les immeubles) et MIDI (système d'information du Service des migrations) ont requis le concours du Bureau, mais dans le second cas uniquement sur la question de l'accès en ligne de l'organe d'exécution, soit le Service des étrangers et des naturalisations de la Police cantonale. Les bases légales nécessaires au projet GRUDIS sont en cours d'élaboration, et l'on est en train de définir les droits d'accès. S'agissant du raccordement en ligne au système MIDI, il n'y a pas lieu de compléter les normes en vigueur étant donné qu'aucune procédure d'appel n'est prévue. Il convient toutefois de garantir que la Police cantonale, en sa qualité d'organe d'exécution en matière de police des étrangers, n'utilise le raccordement en ligne que dans ce domaine.
Dans le cas des projets informatiques suivants, le Bureau n'a pu s'enquérir de la prise en compte des exigences de la protection des données qu'une fois l'autorisation de crédit octroyée: BESIS-2+ (systèmes informatiques des trois cliniques psychiatriques), ABC+Q (programme d'assurance qualité de l'aide ambulatoire aux toxicomanes dans le canton de Berne), installation de caméras vidéo aux établissements de Hindelbank, système de gestion des documents de la Direction des travaux publics, des transports et de l'énergie, système visant à introduire des cartes de légitimation électroniques pour les étudiants et le personnel de l'Université de Berne, FABER/FAK (adaptation de l'infrastructure informatique de l'Office de la circulation routière et de la navigation en vue de l'introduction du nouveau registre des autorisations de conduire ainsi que de permis de conduire lisibles par machine au format des

cartes de crédit), système informatique du laboratoire du Centre de réadaptation de Heiligenschwendi.
Le traitement des prises de position des services contactés par le Bureau n'est pas encore achevé, sauf en ce qui concerne l'installation de caméras aux établissements de Hindelbank. Si des consignes détaillées de qualité ont été produites par un service, il n'en est pas allé de même dans les autres cas: les directives comportaient des lacunes, quand elles ne faisaient pas totalement défaut jusqu'à l'intervention du Bureau. Les ressources requises par le suivi sont considérables (cf. ch. 3.4.2). L'attention du Bureau a été attirée par une commune concernée sur le vaste projet GERES de l'Intendance des impôts, qui en est au stade de l'analyse préliminaire. Ce projet, qui vise à offrir aux communes une plate-forme cantonale de contrôle central des habitants, a été lancé dans la perspective d'une cyber-administration ainsi que du recensement de la population de 2010 notamment.

3.4.2 Stratégie de traitement des projets

La préparation de la huitième Conférence suisse des commissaires à la protection des données, organisée par le canton de Berne, a été l'occasion de réfléchir au traitement des projets informatiques (cf. ch. 3.1.2). L'enquête effectuée à ce propos (cf. ch. 3.4.1) a confirmé l'existence des problèmes évoqués par les orateurs à l'occasion de la conférence: les consignes relatives au déroulement des projets ne tiennent qu'insuffisamment compte des exigences de la protection des données, ou alors elles ne sont pas observées. Il s'agit là d'une tendance qui doit impérativement être contrée.
Les coûts de la prise en considération des impératifs de la protection des données augmentent selon une courbe exponentielle avec l'avancement des projets. Cependant, le Bureau ne dispose ni de connaissances techniques suffisantes dans le domaine de l'informatique, ni des ressources nécessaires pour assurer le suivi des projets. Il devrait donc appartenir aux organes de direction des projets de recourir à des spécialistes externes, la tâche du Bureau se limitant à contrôler le respect de cette obligation.
En tout état de cause, des contrôles a posteriori des systèmes en exploitation de même que le refus d'octroyer des crédits par les organes compétents lorsque l'examen de la protection des données a été omis devraient amener les responsables de projets à considérer qu'il vaut la peine de tenir compte d'emblée des exigences de la protection des données.
Le fait que de telles revendications aient été formulées, lors de la huitième Conférence suisse des commissaires à la protection des données, par des responsables de la sécurité informatique et des personnes chargées de diriger des projets informatiques montre bien à quel point une intervention s'impose. Depuis lors, l'association des Commissaires suisses à la protection des données s'est déclarée favorable au remaniement des consignes HERMES applicables au déroulement de projets.

3.5 Internet et cyber-administration

Le guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail publié par le préposé fédéral à la protection des données répond à la question récurrente, dans le canton de Berne également, de savoir combien de temps les fichiers de journalisation (log-files) des accès à Internet peuvent être conservés par l'employeur: le délai est de quatre semaines. Par contre, il est de six mois pour les paramètres de communication conservés par les fournisseurs de services de télécommunication concessionnaires (loi fédérale sur la surveillance de la correspondance par poste et télécommunication). En tout état de cause, les consignes doivent encore être mises en pratique par les employeurs.
L'Intendance des impôts concrétise, avec l'ordonnance sur la procédure de taxation des personnes physiques, la base légale en vigueur qui autorise le dépôt des déclarations d'impôt par le biais d'Internet. Cependant, le recours à cette possibilité présuppose toujours l'envoi par courrier ordinaire d'un formulaire de validation muni d'une signature manuscrite. Il en résulte une certaine contradiction par rapport au fait que les contribuables peuvent désormais remplir leur déclaration directement sur le serveur de l'Intendance des impôts. En effet, l'existence d'une telle possibilité implique une procédure sûre d'authentification des usagers, qui disposent à tout le moins d'une liaison cryptée avec le serveur authentifié de l'Intendance des impôts excluant toute écoute ou copie par des tiers. En cela, le site Internet de l'Intendance des impôts se distingue positivement de ceux d'autres services cantonaux qui incitent les usagers à leur transmettre sans cryptage des données particulièrement dignes de protection. En tout état de cause, il est nécessaire que les services cantonaux appréhendent le problème du transfert de données de manière unitaire.
Des consignes de sécurité uniformisées s'imposent également pour les sites Internet de la cyber-administration. L'Office fédéral allemand pour la sécurité en matière de technologies de l'information propose à cet égard un document détaillé sur Internet.
L'autorisation d'exploiter les systèmes de traitement des données de la Police cantonale ne prend pas encore position au sujet de la diffusion de données de la police sur Internet (p. ex. avis de recherche, cf. ch. 3.8.1).
La commune de Zollikofen a soumis son site Internet au Bureau pour examen. Cet effort réjouissant, dicté par le souci de suivre une procédure correcte, n'a pu être soutenu qu'au prix d'un travail considérable, notamment en raison de la conjonction de questions de sécurité relevant de la technique informatique d'une part et de questions juridiques précises dans plusieurs domaines spécifiques d'autre part (p. ex. admissibilité de la collecte de données destinées au contrôle des habitants).
D'entente avec les personnes concernées, le collège secondaire de Täuffelen a diffusé pendant deux semaines sur Internet des images vidéo prises toutes les 15 secondes dans une salle de classe. Cet exemple montre bien à quel point il est aisé, même avec peu de moyens, de porter atteinte aux droits de la personnalité.

3.6 Législation

Se fondant sur les propositions de l'association des Commissaires suisses à la protection des données, le Bureau a pris part, au niveau cantonal, à la procédure de participation relative à six lois fédérales. Dans le cas de la loi fédérale sur les services de certification dans le domaine de la signature électronique, il s'est agi d'attirer l'attention sur l'importance de disposer de composants sûrs (claviers, lecteurs de cartes), au bénéfice d'un certificat délivré par une instance officielle. En l'absence de tels composants, les personnes concernées n'accepteront pas de prendre des risques. S'agissant de la révision partielle de la loi fédérale sur la protection des données, la suppression de l'obligation faite aux cantons de tenir un registre des fichiers a été demandée: ce point revêt une importance particulière pour un canton comme celui de Berne, qui applique le principe de la publicité, tant il est vrai que dans son cas la charge de travail considérable liée à la tenue d'un tel fichier est disproportionnée par rapport à l'utilité de ce dernier; il existe en effet, d'une manière générale, une obligation de fournir des renseignements sur le traitement des données à toute personne intéressée qui en fait la demande. Par ailleurs, la nouvelle possibilité offerte aux autorités cantonales de surveillance de recourir contre des mesures de mise en œuvre du droit fédéral est accueillie avec satisfaction, mais l'on ne saurait sous-estimer la question de son intégration dans le droit procédural cantonal. Quant à l'avant-projet de Code de procédure pénale suisse, il renvoie à la réglementation sur les analyses d'ADN qui est contenue dans la loi fédérale sur l'utilisation de profils

d'ADN. Or, cette dernière n'a jamais fait l'objet d'une procédure de consultation ordinaire, et il convient d'attirer une nouvelle fois l'attention sur ses lacunes, soit l'absence d'une liste des infractions et le fait que l'effacement d'office du profil d'ADN ne soit pas généralisé. En ce qui concerne les actes législatifs cantonaux, il est renvoyé aux chiffres 3.2.5 (loi sur la BEDAG Informatik) et 3.5 (ordonnance sur la procédure de taxation des personnes physiques: dépôt des déclarations d'impôt par le biais d'Internet).

3.7 Collectivités de droit communal

Une première ébauche sommaire de guide destiné aux autorités communales de surveillance de la protection des données a pu être achevée, en réponse à une demande formulée par diverses instances, et sera publiée sur le futur site Internet de la Direction de la justice, des affaires communales et des affaires ecclésiastiques. Ce guide s'adresse aux communes de plus de 5000 habitants – les seules dont on peut admettre qu'elles bénéficient d'un suivi en tout cas partiellement professionnel. Il s'est par contre avéré impossible, dans un premier temps, de rédiger l'ensemble des consignes en un document utilisable par des organes de surveillance de milice. En matière de sécurité informatique, il est renvoyé au manuel de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (IT-Grundschutzhandbuch) disponible en allemand et en anglais sur Internet. Par contre, la version française de ce manuel qui serait nécessaire dans le canton de Berne fait défaut.
Un cours a pu être organisé en collaboration avec les autorités de surveillance de la protection des données de deux grandes communes.
Une personne concernée par un dossier a saisi le préfet d'un recours administratif pour faire valoir son droit à consulter les procès-verbaux des commissions et du conseil communal.
La communication de données concernant des demandeurs d'asile lors d'une assemblée communale a été à l'origine d'une procédure pénale contre un membre d'une autorité prévenu de violation de l'obligation de garder le secret; depuis lors, l'action publique a été suspendue.
Ce n'est que suite à un arrêté du conseil communal qu'un service social communal a mis fin à une pratique qui consistait à charger un détective privé de s'assurer que certains bénéficiaires d'une aide sociale y avaient bel et bien droit.
Il est renvoyé au chiffre 3.5 en ce qui concerne la webcam installée au collège secondaire de Täuffelen et le site Internet de la commune de Zollikofen.
Se demander si les responsables doivent connaître les conditions générales du traitement des données est, au vu des exemples qui précèdent, une question rhétorique. D'ailleurs, les cours de formation et de perfectionnement proposés ont été bien fréquentés. Il existe encore une demande de soutien juridique de la part des responsables de l'accomplissement de tâches supra-communales notamment, comme dans le cas des centres de puériculture ou encore des centres de consultation pour problèmes de dépendance.

3.8 Points abordés dans le rapport précédent

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

Le Conseil-exécutif a délivré son autorisation d'exploiter les systèmes de traitement des données de la Police cantonale en janvier. En réponse à la proposition de la Direction de la police et des affaires militaires, les accès au sous-système OBORA doivent être journalisés. De plus, un organe spécialisé indépendant doit s'assurer tous les deux ans que la protection et la sécurité des données sont garanties. A cet égard, ce sont les exigences en matière de sécurité informatique valables dans l'administration cantonale qui s'appliquent (cf. ch. 3.3.1). L'autorisation d'exploitation vaut pour les principaux systèmes, et la question de savoir si d'autres systèmes de traitement des données de la Police cantonale requièrent une autorisation d'exploitation est actuellement à l'étude (site Internet, systèmes vidéo, centrale des amendes d'ordre, systèmes de traitement des données exploités en collaboration avec la Confédération).

3.8.2 Consignes en matière de sécurité informatique

Cf. chiffre 3.3.1

3.8.3 Sécurité du courrier électronique

Cf. chiffre 3.3.2

3.8.4 ADN

Les services cantonaux transmettent eux aussi les profils d'ADN établis à des fins de poursuite pénale à la banque de données exploitée par la Confédération, en application de l'ordonnance fédérale sur le système d'information fondé sur les profils d'ADN qui restera en vigueur jusqu'à fin 2004 seulement. L'avant-projet de Code de procédure pénale suisse renvoie à la réglementation sur les analyses d'ADN qui est contenue dans la loi fédérale sur l'utilisation de profils d'ADN dont il était question dans le précédent rapport (cf. ch. 3.6). Le Bureau partage l'avis exprimé dans la réponse à la motion Rytz selon lequel il ne reste guère de marge au canton pour légiférer compte tenu des nouvelles compétences qu'a la Confédération d'édicter des normes de procédure pénale (réforme de la justice) et des travaux législatifs entrepris au niveau fédéral.

3.8.5 Contrôles du traitement des données informatiques

Cf. chiffre 3.2.5

3.9 Cas particuliers

3.9.1 Vidéo

La ville de Bienne a fait installer des caméras vidéo destinées à la surveillance du trafic et des places de stationnement, sans toutefois que les images ne soient enregistrées. A Berne, les autorités communales compétentes discutent de l'opportunité d'une vidéosurveillance et, le cas échéant, des modalités de cette dernière. Une entreprise de transport a soumis au Bureau un projet d'installation de caméras vidéo dans les trains semblable au projet pilote des CFF dans la région de Genève. L'Office fédéral des routes oblige tous les cantons à faire surveiller les tunnels autoroutiers d'une certaine longueur au moyen d'installations vidéo dotées d'un système de détection des événements. Dans le canton de Berne, les images sont transmises aux centres d'entretien de l'Office des ponts et chaussées de même qu'à la Centrale d'engagement de la Police cantonale; elles sont également enregistrées, du moins en cas d'événements particuliers. Une commune a équipé son nouveau parking couvert d'une installation vidéo et s'est enquise des bases légales nécessaires. Tandis qu'une école examinait simplement l'opportunité d'une vidéosurveillance des abris pour vélos, assortie d'un enregistrement des images, un collège secondaire a fait placer une webcam dans une salle de classe pour une durée limitée

(cf. ch. 3.5). Un organe communal de police industrielle a demandé quelles étaient les conditions légales à respecter pour qu'un détenteur de taxi puisse établir une image électronique de chaque client. S'il a été possible en l'espèce de le renvoyer pour l'essentiel à l'aide-mémoire du préposé fédéral à la protection des données sur la vidéosurveillance effectuée par des personnes privées, il s'est agi dans les autres cas évoqués plus haut de souligner la nécessité d'une base légale – à tout le moins pour la conservation des images. Au niveau cantonal, il existe une base légale concernant l'enregistrement d'images et de sons lors de manifestations de masse dans la loi sur la police ainsi que dans l'ordonnance sur les enregistrements vidéo qui en découle. D'autres bases légales font défaut au niveau cantonal de même que, le plus souvent, au niveau communal. L'édiction de telles bases ne doit pas uniquement régler la question du recours à la vidéosurveillance, mais également en préciser les conditions: but, durée de conservation des images, mesures de sécurité, publication et exploitation d'autres possibilités techniques telles que la détection des événements, ce dernier point étant d'une actualité toute particulière au vu de la rapidité de l'évolution technologique.

3.9.2 Enquêtes auprès du personnel et autres enquêtes

Les enquêtes se multiplient, notamment dans le cadre de la nouvelle gestion publique. Il y a régulièrement lieu de relever que les questionnaires doivent mentionner la base légale sur laquelle ils se fondent, le but de l'enquête ainsi que le caractère facultatif de la participation.

Préalablement consulté au sujet de l'enquête sur la satisfaction du personnel, le Bureau a pu trouver, d'entente avec les responsables du projet, des solutions respectant les exigences de la protection des données. A cet égard, les discussions ont avant tout porté sur l'anonymisation, le moment de la destruction des données, la collecte auprès des membres du personnel de données relatives à leurs supérieurs hiérarchiques, ainsi que sur l'espace destiné aux remarques. La loi sur la protection des données confère aux personnes concernées un droit de consulter leurs données et d'obtenir des renseignements. Il est donc inadmissible de promettre la confidentialité des réponses aux personnes interrogées lorsqu'on collecte auprès d'elles des données sur des tiers reconnaissables (en l'espèce leurs supérieurs hiérarchiques). Ce mode de faire s'oppose en outre au principe selon lequel les données doivent d'une manière générale être collectées auprès des personnes directement concernées. De telles limites doivent également être observées lorsqu'il est prévu de laisser un champ libre pour les remarques dans un questionnaire.

18 janvier 2002

Le délégué à la protection des données: *Siegenthaler*