Rapport d'activité 2018 du Bureau pour la surveillance de la protection des données du canton de Berne

Bureau pour la surveillance de la protection
des données du canton de Berne
Poststrasse 25
3072 Ostermundigen
Téléphone 031 633 74 10
Télécopie 031 634 51 53
protectiondesdonnees@be.ch
www.be.ch/bpd

Table des matières

1 Introduction

1.1 2018 en bref

Le 8 janvier 2019, le Conseil-exécutif a arrêté le programme de législature 2019 à 2022 et a défini son engagement à l'horizon 2030. Il s'est alors notamment fixé comme objectif d'exploiter les opportunités de la transition numérique et de fournir à la population et à l'économie des services efficaces, de haute qualité et efficients. Le 5 mars 2019, la direction opérationnelle de la cyberadministration suisse et le Secrétariat d'Etat à l'économie ont publié la deuxième étude nationale sur la cyberadministration. Cette enquête représentative a été conduite auprès de la population, des entreprises et des administrations suisses. Parmi les résultats obtenus, il ressort que 68 pour cent de la population fait confiance aux autorités cantonales qui fournissent des prestations en ligne pour la protection de la personnalité et des données. Ce taux correspond peu ou prou à la valeur obtenue dans la première étude, publiée en novembre 2017. Cette dernière indiquait parallèlement que les autorités cantonales estimaient à 95 pour cent la part de la population ayant confiance en elles pour le traitement des données fournies en ligne. Si la question était posée au sujet du traitement électronique des données à l'intérieur de l'administration, les résultats seraient probablement similaires; il faudrait ainsi constater le même écart qu'à l'exercice précédent entre ce que les Suisses et Suissesses ressentent vraiment et ce que les administrations s'imaginent. Il est donc essentiel que les autorités cessent de considérer la protection et la sûreté des données comme un simple cadre légal et, en ce sens, comme un frein à la révolution numérique pour les apprécier par ailleurs comme le sésame de l'acceptation et de la réussite des prochains développements de la cyberadministration.

Dans ce contexte, les diverses tâches qui ont occupé le Bureau pour la surveillance de la protection des données (le Bureau) en 2018 – à savoir le contrôle des applications informatiques utilisées (ch. 3), le contrôle préalable des installations de vidéosurveillance (ch. 4) et de projets informatiques divers (ch. 5), les avis exprimés à la demande des autorités cantonales et des communes (ch. 6) et lors de la préparation des actes législatifs (ch. 7) ainsi même que l'évolution des procédures de recours administratif et judiciaires (ch. 8) – ne doivent pas être uniquement perçues comme des composantes de l'activité de surveillance de l'administration prévue par le législateur, puisqu'il s'agit aussi de prestations dont elle tire profit.

1.2 Collaboration avec le préposé fédéral à la protection des données et à la transparence et les commissaires suisses à la protection des données (privatim)

Le Bureau a participé à une séance de travail du groupe de coordination au moyen duquel le préposé fédéral à la protection des données et à la transparence (PFPDT) coordonne la surveillance du Système d'information Schengen (SIS). L'Office fédéral de la police (fedpol) n'a pas envoyé suffisamment tôt les fichiers journaux des requêtes de la police cantonale bernoise, de sorte que le Bureau n'a pas pu procéder à la vérification prévue. Etant donné que d'autres cantons ont vécu une expérience du moins partiellement identique, le groupe de coordination du PFPDT a décidé d'exiger de fedpol une procédure claire et uniforme.

Les collaborateurs du Bureau ont œuvré dans plusieurs groupes de travail de privatim et ont participé à un atelier sur les prérequis des services infonuagiques. Le groupe de travail «Administration numérique» a traité durant plusieurs séances divers thèmes touchant à la cyberadministration, plus précisément aux exigences liées aux portails en ligne, aux projets fédéraux concernant l'identité électronique (E-ID) et au vote électronique. Un guide pour les portails web a été publié en 2018: http://www.privatim.ch/fr/publications.

Comme en 2017, le groupe de travail «Santé» s'est intéressé à la protection des données et à la sécurité du dossier électronique du patient. Les compétences en matière de protection des données ont été discutées en début d'année, lors d'une séance qui s'est déroulée avec l'Office fédéral de la santé publique et le PFPDT. A la date du présent rapport, l'épineuse question de la délimitation des compétences n'avait pas encore été réglée. Le manque de ressources a forcé les collaborateurs du Bureau à suspendre leur participation au groupe de travail «Santé» depuis mars 2018 jusqu'à nouvel avis.

1.3 Modifications intervenues dans le droit supérieur

En raison des obligations de la Suisse découlant des accords d'association à Schengen, la directive (UE) 2016/680, adoptée au niveau européen en avril 2016, devait être mise en œuvre dans l'ensemble du pays au 1er août 2018 au plus tard. Cette directive – relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données – a été introduite dans le droit cantonal par

l'édiction d'une ordonnance urgente dont la validité est limitée à quatre ans (ordonnance du 4 juillet 2018 portant introduction de la directive (UE) 2016/680 relative à la protection des données à caractère personnel). Berne a donc été le deuxième canton à satisfaire à ses obligations. Seul le canton d'Argovie a réussi à réviser sa loi sur la protection des données dans les délais. Les deux cantons ont rempli leur mission avant la Confédération, dont la loi sur la protection des données Schengen est entrée en vigueur le 1er mars 2019. A présent, il s'agit de transposer la teneur de l'ordonnance urgente dans le droit ordinaire à l'occasion d'une révision de la loi cantonale sur la protection des données (LCPD), qui doit moderniser l'ensemble des prescriptions en la matière.

2 Description des tâches, priorités et moyens à disposition

2.1 Priorités

Selon l'article 34 LCPD, le Bureau doit notamment surveiller l'application des dispositions sur la protection des données, contrôler la sécurité des données, procéder au contrôle préalable des projets informatiques, conseiller l'administration (actes et exécution) et les personnes concernées, ainsi que le cas échéant jouer le rôle d'intermédiaire entre les autorités et les particuliers. Si la loi place toutes les tâches sur un pied d'égalité, le Bureau est obligé, vu les ressources humaines et financières disponibles, de traiter les affaires selon un ordre des priorités. En 2018, ce dernier a été établi selon les critères suivants:

– Préséance de l'autorité compétente: ce sont les autorités communales de surveillance en matière de protection des données ou les services juridiques de l'administration cantonale compétents qui conseillent les services administratifs communaux et cantonaux. S'agissant des questions communales, les autorités communales de surveillance en matière de protection des données conseillent les personnes concernées. Il convient de renvoyer toute personne ou tout service qui adresse une demande directe au Bureau à l'autorité compétente. Ces compétences, et le tri des requêtes qu'elles impliquent, sont inscrites dans l'ordonnance sur la protection des données.

– Standards de qualité différenciés: lorsqu'il s'agit de répondre à une personne ou à une autorité non professionnelle, le Bureau peut se contenter d'envoyer des instructions (sans arguments juridiques). En revanche, lorsqu'il doit prendre position au sujet de documents émanant d'une autorité de justice, une réponse détaillée et approfondie d'un point de vue juridique est nécessaire. Le standard de qualité doit être défini au préalable.

– Subsidiarité de l'activité de surveillance: la législation sur la protection des données donne aux personnes concernées des moyens efficaces pour se défendre (celles-ci peuvent notamment demander la rectification, la destruction ou la constatation du traitement illicite de données personnelles). L'autorité de surveillance n'a pas à intervenir lorsque de telles possibilités sont offertes. Les personnes concernées doivent toutefois être informées de leurs droits. S'il y a lieu de croire que des problèmes de fonctionnement existent, l'autorité de surveillance doit engager les moyens nécessaires (p. ex. contrôles) au suivi de ces problèmes.

– Contrôles préalables: les consignes applicables aux contrôles préalables visent à inciter les responsables de projet à mettre en œuvre les prescriptions en matière de protection des données. Cet objectif peut être atteint même si le Bureau se contente d'une vérification formelle du dépôt des documents assortie ou non d'un examen partiel du contenu. Celui-ci peut renoncer totalement à un tel examen si un responsable de projet lui a déjà soumis à plusieurs reprises des documents qui étaient en ordre, si un projet a une importance secondaire ou si sa charge de travail globale ne lui permet pas de procéder aux examens dans les délais. Il y a notamment lieu de procéder à des contrôles partiels lorsque, dans certains domaines, des constats peuvent être tirés de précédents examens (p. ex. sur la sécurité de l'infrastructure informatique utilisée) ou lorsque certains domaines sont connus pour présenter des risques importants (p. ex. droits d'accès à des données personnelles particulièrement dignes de protection).

– Renonciation à prendre position au sujet d'actes législatifs fédéraux: dans la procédure législative, les mêmes questions se posent régulièrement en termes semblables pour tous les cantons. Pour ces questions, le Bureau se contente de diffuser la prise de position de privatim et, le cas échéant, de participer à l'élaboration de celle-ci.

Les tâches étaient attribuées aux collaborateurs en fonction de la région (communes), de l'unité administrative cantonale (Direction) et du domaine (p. ex. droit cantonal sur les Eglises). Ceux-ci fixaient eux-mêmes les priorités en fonction des critères susmentionnés. La priorisation des affaires relatives aux contrôles préalables s'effectuait en collaboration avec la direction du Bureau. Si les collaborateurs ne parvenaient plus à respecter les délais de réponse fixés (conformément aux objectifs de prestation de NOG), certaines priorités pouvaient être déplacées, le dossier pouvait être confié à un autre collaborateur, le traitement d'un dossier pouvait être (partiellement) abandonné ou le standard de qualité

revu à la baisse, avec l'accord de la direction du Bureau. Celle-ci garantissait toutefois que les applications informatiques faisaient dans tous les cas l'objet d'un contrôle, que le suivi des contrôles était assuré et que, même s'il était renoncé à certains contrôles préalables, les responsables de projet veillaient par eux-mêmes au respect de la protection des données. S'agissant des conseils dispensés et des interventions réalisées en qualité d'autorité de surveillance, l'accent a surtout été mis sur les évolutions techniques qui ont des conséquences particulières sur les droits de la personnalité.

2.2 Personnel et finances

Le Bureau disposait de 5,15 postes à temps plein (tâches de secrétariat comprises) et les charges d'exploitation étaient de 149 milliers de francs, dont 119 étaient affectés à l'examen des applications informatiques par des services externes.

En octobre, le Bureau a quitté ses locaux du centre-ville de Berne pour emménager à Ostermundigen. Ce déménagement et l'introduction parallèle d'un nouveau logiciel de gestion des affaires ont été à l'origine de l'archivage de l'ensemble des documents sur papier du Bureau. Etant donné que les Archives de l'Etat de Berne les ont presque tous considérés comme ayant une valeur archivistique, le Bureau a livré 21,6 mètres linéaires de papier pour archivage ou préarchivage; tous les documents de 1991 à 2014 étaient réunis dans 216 boîtes d'archives. Depuis août, le papier n'est plus le principal support des dossiers du Bureau, qui a donné la primauté au numérique. Dans le nouveau système GEVER, la valeur archivistique est prédéfinie pour chaque affaire, ce qui réduira largement la charge de travail pour le versement (électronique).

3 Contrôle des applications informatiques utilisées

Quatre audits ont été réalisés:

– Contrôle de l'application infonuagique Microsoft 365 de la Direction de l'instruction publique (INS)

Les services informatiques de l'INS mettent à la disposition des écoles qui le souhaitent une infrastructure en nuage pour les cours. Le cadre légal est fixé dans un contrat qui a été élaboré et conclu spécialement à cette fin avec Microsoft Suisse.

L'examen a révélé une claire répartition des responsabilités relatives à l'exploitation et l'utilisation. L'INS et Microsoft assument ensemble la mise à disposition de l'infrastructure et la prestation de services, gestion des utilisateurs compris. Les écoles, pour leur part, sont responsables du contenu des données généré par l'utilisation des applications et des systèmes. Il n'existait jusqu'alors pas de règlement définissant les modalités d'utilisation et les attributions.

Le contrôle a en outre montré que le traitement des données particulièrement dignes de protection dans l'application infonuagique, pour qu'il réponde aux normes légales, requiert de la part des utilisateurs une discipline stricte.

Les responsables de l'INS se sont montrés très coopératifs vis-à-vis des constations faites et ont pris les mesures qui s'imposaient pour combler les lacunes dans les plus brefs délais.

– Protection de base du Centre psychiatrique Münsingen SA (CPM)

Le Bureau a contrôlé avec l'aide d'un organe externe l'infrastructure informatique de base du CPM. Il a constaté que les responsables de l'exploitation opérationnelle des ressources informatiques déployaient de gros efforts afin de garantir, autant que faire se peut, un traitement des données très sensibles de leur institution qui soit conforme aux règles de la protection des données.

Pendant l'examen, de graves défauts ont cependant été constatés eu égard à la protection des données et à la sûreté de l'information. Ils résultent principalement du manque de prescriptions stratégiques et tactiques. Il n'existe par exemple pas de prescription sur le modèle d'une norme reconnue comme la norme ISO 27001 / 27002 propre à servir de base à la définition et à la mise en œuvre de mesures ainsi qu'à la vérification de leur efficacité. L'attribution et la délimitation des responsabilités méritent aussi un remaniement notamment dans les domaines des droits d'accès, des applications ou des fichiers.

Les constatations décrites ont été analysées avec le Bureau. Cette collaboration a donné jour à un plan de mesures, qui est mis en œuvre.

– Examen de la protection de base de l'infrastructure informatique de la Police cantonale (POCA)

L'infrastructure informatique de la POCA, qui est complexe, a fait l'objet d'un examen. Portant sur la mise en œuvre des prescriptions de la protection de base, le contrôle devait montrer dans quelle mesure l'infrastructure de l'exploitation actuelle était conforme aux prescriptions SIPD et ainsi diminuer le travail nécessaire lors des prochains contrôles préalables. Le premier contrôle a donné lieu à d'importantes contestations. Les points soulevés dans le rapport de l'organe externe de contrôle ont été traités en étroite collaboration avec les responsables, les mesures requises ont pu être planifiées dans les meilleurs

délais et partiellement appliquées. Un contrôle de suivi a ainsi pu être conduit en décembre.

– Sûreté de l'information dans le traitement des données par l'hôpital universitaire de Berne au moyen d'appareils mobiles

Il a été difficile de procéder au contrôle de l'infrastructure. D'une part, les interlocuteurs désignés auparavant dans le programme d'audit (y c. partenaires externes) n'étaient pas disponibles; d'autre part, les entretiens ont souvent révélé de grandes failles dans l'infrastructure informatique de base ou dans les processus élémentaires. Ces dernières influencent directement ou indirectement le traitement des données soumis au contrôle et ne peuvent pas être évitées. Les résultats de l'examen ont mal été acceptés par le service concerné. Le rapport d'audit a été transmis au directoire de l'institution en décembre. Le Bureau attend de sa part une attitude coopérative afin que les mesures urgentes visant à rendre l'exploitation conforme aux exigences de la protection des données puissent être définies, planifiées et mises en œuvre rapidement. Les conclusions du rapport suggèrent qu'un examen complet des infrastructures de base et des processus informatiques est nécessaire.

4 Vidéosurveillance

Plusieurs installations de vidéosurveillance situées dans des bâtiments cantonaux ont fait l'objet d'un contrôle préalable. Parmi celles-ci se trouvent notamment les installations du Groupe de l'Ile (maternité de l'hôpital de l'Ile / périmètre d'évolution 6.1; unité cérébrovasculaire de l'Hôpital de l'Ile; hôpital de Riggisberg). Le Bureau a aussi évalué à titre préliminaire des projets en préparation et leur admissibilité d'après les bases légales (enregistrement des entretiens des organismes régionaux de placement [ORP] de l'Office de l'économie bernoise [beco]; surveillance de l'Institut de médecine légale et de l'aire d'Engehalde de l'Université de Berne). Il a élaboré des modèles présentant les points à vérifier lors du contrôle préalable des installations de vidéosurveillance qui ne sont pas prévues par la loi sur la police mais par des lois spéciales ainsi que lors des contrôles préalables effectués par les autorités communales de surveillance.

Tous les projets ne sont pas admissibles en la forme proposée: les enregistrements constituent une infraction majeure au droit fondamental à la protection des données et nécessitent une base légale formelle claire. A défaut d'une telle base, seule la surveillance en temps réel, dans la mesure où elle est nécessaire à l'accomplissement des tâches, est permise. Les enregistrements dans les hôpitaux et l'Institut de médecine légale ne sont pas admis dès lors qu'ils ne se fondent ni sur la loi sur la police (ils ne revêtent pas de but policier, il ne s'agit pas de bâtiments ou locaux librement accessibles au public) ni sur une autre loi (aucune réglementation dans la loi sur les soins hospitaliers ni dans la loi sur l'Université par exemple). Même s'il vise à l'amélioration de la qualité, l'enregistrement des entretiens entre les collaborateurs de l'ORP et les clients n'est pas admis sans base légale.

Le Bureau rappelle régulièrement aux hôpitaux qu'il convient de demander à l'Office du médecin cantonal de lever l'obligation de garder le secret avant la transmission à la Police cantonale d'images sur lesquelles figurent des patients.

Le Bureau est aussi parvenu à la conclusion que l'utilisation de caméras de surveillance par le secteur Protection contre les immissions du beco pour détecter d'éventuelles émissions de fumée non autorisées doit être explicitement prévu dans l'ordonnance cantonale sur la protection de l'air.

5 Contrôle préalable de projets informatiques

Le Bureau a de nouveau examiné un grand nombre de projets informatiques. La liste suivante n'est pas exhaustive, elle ne fait que donner des exemples d'examens en cours ou achevés.

5.1 Contrôles préalables en cours

– BE-GEVER

En vue de l'introduction du nouveau système de gestion électronique des affaires (BE-GEVER) à l'échelle cantonale, le Bureau a déjà demandé et reçu pour le contrôle préalable les concepts SIPD de différents offices et services pour chaque mandant en 2017. Le Bureau a recommandé l'utilisation d'une double authentification pour la sécurisation de l'accès aux systèmes et le recours à une signature électronique des documents. Il a aussi formulé une recommandation motivée à l'intention de quatre offices de la Direction des finances (FIN). Cette dernière a décidé de s'occuper de leur traitement et de l'interrompre jusqu'au jugement du recours par le Tribunal administratif (100.2017.72U; cf. ch. 8). En mars, le Bureau a retiré les recours de droit administratif formés contre ces décisions et a exigé que des mesures soient prises immédiatement pour combler les lacunes de BE-GEVER.

A deux reprises (pour BE-GEVER en général et pour une gestion mobile des séances de la Direction de la santé publique et de la prévoyance sociale [SAP]), le Bureau a formé un recours administratif auprès de la FIN en novembre 2018, car l'Office d'informatique et d'organisation (OIO) avait rendu des décisions rejetant les recommandations motivées (art. 35, al. 4 LCPD) qu'il avait pourtant adressées à la SAP en invoquant la

nouvelle ordonnance sur les technologies de l'information et de la communication de l'administration cantonale (OTIC).

– Système de gestion Competella

Le Bureau a répondu à la demande d'un tiers concernant le système de gestion Competella, une prestation TIC de base fournie par l'OIO aux autorités judiciaires ou administratives cantonales. Le système permet une analyse complète des données de téléphonie secondaires (p. ex. qui parle avec qui et pour combien de temps; quel appel avec quelle personne aboutit à quelle vitesse ou n'aboutit pas; quel appel est interrompu). Etant donné qu'une telle analyse relève dans une grande mesure de la protection des données du personnel cantonal mais aussi des clients, le Bureau a fait parvenir une requête relevant du droit de la surveillance auprès de l'office compétent. Il demandait des renseignements sur l'utilisation du système en vue du contrôle préalable. L'OIO a ensuite informé les utilisateurs de la nécessité du contrôle préalable et leur a recommandé de renoncer, jusqu'à ce qu'il soit fait, à recourir à la fonction d'évaluation sans la base légale requise.

– Arrêts domiciliaires sous surveillance électronique

L'application Electronic Monitoring (EM) permet à l'Office de l'exécution judiciaire (OEJ), conformément au droit fédéral, d'exercer une surveillance électronique sur les peines privatives de liberté prononcées contre des adultes et des adolescents ainsi que sur des mesures ambulatoires (p. ex. arrêts domiciliaires). Toutes les données sont particulièrement dignes de protection. Le canton de Berne a adopté la solution logicielle du canton de Zurich au 1er janvier. La mise en service d'une solution nationale est prévue le 1er janvier 2023 au plus tard. La loi sur l'exécution judiciaire et ses actes d'exécution ont créé les bases légales nécessaires au traitement, à la conservation et à la destruction des données (cf. ch. 7.2). Le contrôle préalable des documents remaniés n'est pas encore achevé.

– Progiciel de gestion intégré (PGI)

Le projet cantonal PGI doit offrir un système de soutien dans le domaine des finances, du personnel et de la logistique. L'OIO s'est déjà adressé au Bureau lors de la phase conceptuelle pour de premiers conseils. La question centrale portait sur les exigences qu'une solution infonuagique posait.

– Programme de gestion des personnes détenues (système Gina)

La réalisation du projet Fabesys a été concrétisée par l'introduction de l'application web Gina par l'OEJ. Le système utilisé jusqu'alors est ainsi remplacé par une solution web axée sur le déroulement des processus. Le contrôle préalable a pu être mené en plusieurs étapes et était presque terminé à fin 2018.

– Plate-forme GERES

Le contrôle préalable du registre cantonal des personnes (GERES) géré par l'OIO a entre autres révélé que l'accès par Internet et Citrix devait dépendre d'une double authentification. Il faut encore apporter la preuve de la conservation des données et des historiques conforme aux principes de la protection des données, de la protection des données des personnes exposées, qui fait encore défaut (art. 14 LCPD), ainsi que des mesures techniques prises pour empêcher tout accès abusif aux données.

– NewParePas

Le contrôle préalable d'une application de la Direction de la justice, des affaires communales et des affaires ecclésiastiques pour la gestion des paroisses et des postes d'ecclésiastique était sur le point d'être achevée à la fin de l'année.

5.2 Contrôles préalables achevés

Les procédures de contrôle préalable suivantes ont pu être achevées:

– Services de base du WLAN

Les documents SIPD relatifs au projet ont été adaptés par l'OIO avant de faire l'objet d'un audit mené par une entreprise externe. Se fondant sur le rapport d'audit, l'OIO a rempli les dernières exigences, de sorte que la procédure a pu prendre fin. Du point de vue du Bureau, la sécurité offerte avec la nouvelle technologie SSD «BEdirect» est plus faible qu'avec la solution SSD «BEintern», raison pour laquelle un audit des services de base est prévu en 2019.

– Gestion des relations avec les clients de la Haute école spécialisée bernoise (BFH)

Le nouveau programme de gestion des relations avec les clients (GRC) de la BFH implique l'introduction d'un système de gestion des adresses et d'un système de gestion de campagnes. Les droits d'accès sont accordés à un très large nombre et le volume des données est important. Cependant, aucune donnée personnelle particulièrement digne de protection n'est traitée. Le Bureau juge donc la situation acceptable. Les dernières modifications des documents SIPD relèvent de la seule responsabilité de la BFH.

– eBau

Le contrôle préalable concernant la possibilité de mener la procédure d'octroi du permis de construire par la voie électronique a pris fin à la condition que les quelques charges restantes soient remplies (accès des communes et des autorités

compétentes au moyen de BE-Login, garantie des mesures techniques et organisationnelles pour le traitement conforme au droit de la protection des données par les appareils et corrections dans la matrice des droits d'accès).

– Gestion électronique de dossiers personnels

Le contrôle technique préalable du projet eDossiers s'est fait en plusieurs temps avant que la sûreté de l'information requise ne soit présentée. Le contrôle du projet sous l'angle juridique confirme le fait que les droits d'accès sont aménagés de manière proportionnée. L'organe responsable doit toutefois encore retravailler de lui-même les délais de conservation indiqués dans le document relatif à la conservation, à l'archivage et à la suppression des données.

– eDéménagement

Le système électronique eDéménagement ne requiert pas d'identification à proprement parler, ce que déplore le Bureau. Il est ainsi possible qu'une personne annonce indûment le déménagement d'une autre personne sans que le système électronique ne puisse le détecter. Pour que les données des registres des communes pilotes puissent rester correctes, le Bureau a recommandé le maintien du contrôle d'identité par les communes. L'ordonnance exploratoire sur l'annonce électronique des déménagements, entrée en vigueur au 1er février 2019, ne mentionne pas les prescriptions en vigueur concernant le contrôle d'identité par les autorités communales lors de la phase d'essai (cf. ch. 7.2). Le Bureau a renoncé à émettre une recommandation motivée contre la mise en œuvre de l'ordonnance car la tenue correcte des registres relève des communes et des autorités communales de surveillance.

– Système d'information agricole (GELAN)

En complément du contrôle préalable achevé en 2017, une possible modification des processus d'archivage et de destruction du système d'information agricole des cantons de Berne (représenté par l'Office de l'agriculture et de la nature), de Fribourg et de Soleure a été examinée.

– Système d'informations cliniques (SIC) de l'hôpital régional de l'Emmental (RSE AG)

Le contrôle préalable du SIC de l'hôpital régional de l'Emmental a donné lieu à de nombreux échanges. Après sept prises de position de la part du Bureau, la confirmation de la mise en œuvre des adaptations obligatoires en matière de droit de la protection des données a mis un terme à la procédure. Le Bureau a par exemple convenu avec les responsables du système que les possibilités de recherche de dossiers clos et d'accès pour les médecins assistants (qui travaillent à Berthoud et à Langnau) seraient limitées aux cas qui concernent leur domaine d'expertise.

– Logiciel de sondage en ligne

Le contrôle préalable du logiciel de sondage en ligne proposé par l'OIO a pu être achevé. L'utilisation de l'application nécessitait d'imposer certaines dispositions à l'utilisateur pour la protection des données.

Les procédures achevées qui concernaient des installations de vidéosurveillance sont détaillées au chiffre 4.

6 Avis exprimés, pratique

Les éléments suivants donnent une idée des nombreuses demandes adressées au Bureau:

– Projet de recherche sur la violence domestique

A la demande du Service bernois de lutte contre la violence domestique, le Bureau a exposé les exigences propres au domaine de la protection des données dans le cadre du projet de recherche de la BFH et de la Haute école de travail social du Valais sur les violences domestiques exercées à l'encontre des personnes âgées. Etant donné que le projet inclut la participation des autorités de l'autre canton et d'organisations privées, le traitement des données doit tenir compte des prescriptions des deux cantons participants ainsi que de la Confédération en matière de protection des données.

– Effets du règlement général européen sur les services administratifs et les communes (RGPD)

L'avis du Bureau a souvent été sollicité par les services administratifs et les communes au sujet des effets du règlement européen 2016/679. Le Bureau a donc conçu, avec l'aide de l'Office des affaires communales et de l'organisation du territoire, une information devant servir de repère et fournir des renseignements aux organes intéressés (ISCB 1/152.04/10.4).

– Groupe de travail pour les applications infonuagiques de l'OIO

Le Bureau a participé à plusieurs séances du groupe de travail de l'OIO chargé d'élaborer des normes cantonales uniformes pour l'admissibilité des applications infonuagiques.

– Motion 142-2018 (Gullotti)

Pour la rédaction de la réponse du Conseil-exécutif à la motion Gullotti (Pour une statistique transparente et précise des appartenances religieuses des citoyens/-nes inscrit(e)s au registre des habitants des communes bernoises), le Bureau a indiqué les conditions qui devaient être remplies au regard de la protection des données.

– Effacement des données du système d'information de la police

Le Bureau a répondu aux questions que plusieurs particuliers se posaient à propos de l'effacement des données enregistrées dans le système d'information de la police.

– Surveillance des collaborateurs

Une institution active dans le domaine de la santé qui remplit un mandat public a demandé au Bureau de prendre position sur le règlement d'utilisation des moyens de communication électroniques destiné à ses collaborateurs. Elle y prévoyait entre autres la journalisation du recours à l'infrastructure TIC. Le Bureau a répondu qu'une telle surveillance portait gravement atteinte aux droits fondamentaux et qu'une base légale suffisante était nécessaire. Elle ne peut uniquement se fonder sur un règlement, encore moins invoquer l'accomplissement des tâches légales. La journalisation n'est admise que si elle sert à des tâches telles que la maintenance de la technique et la réparation des défaillances.

– Publication en ligne des procès-verbaux des assemblées communales

Plusieurs communes ont demandé l'avis du Bureau concernant la publication sur Internet des procès-verbaux de leurs assemblées. Selon la loi cantonale sur l'information, les assemblées communales sont publiques. Une publication sur Internet doit être conforme aux prescriptions de la LCPD et de l'ordonnance sur la protection des données (OPD) relatives à la communication de données personnelles à l'étranger, puisque les procès-verbaux peuvent être consultés dans le monde entier. Une base légale au niveau communal s'impose. Sur son site Internet, l'OACOT met à la disposition des communes un modèle d'ordonnance qui a été totalement remanié en 2018. L'autorité communale compétente doit s'assurer que la publication sur Internet n'entraîne aucun risque particulier pour les personnes concernées et que leur personnalité n'est pas gravement menacée par la communication des données à l'étranger. Il convient de garantir la protection des intérêts privés et publics prépondérants, de même que les droits de blocage, d'accès et de rectification. De plus, les informations communiquées sur Internet doivent être traitées techniquement de manière à empêcher les moteurs de recherche de les indexer. Le cas échéant, les adresses de courriel publiées doivent l'être exclusivement sous une forme qui empêche toute lecture par un robot pourrielleur.

– Résultats de l'évaluation de l'aptitude à la conduite

Une personne concernée a estimé que l'envoi des résultats de l'évaluation prévue par la loi de l'aptitude des conducteurs de 70 ans et plus à l'Office de la circulation routière enfreignait le principe du secret médical. La loi sur la circulation routière prévoit toutefois pour ce cas la levée du secret professionnel. Aux termes de la loi, les résultats médicaux sont transmis lorsqu'il existe une maladie ou un état significatifs du point de vue de la médecine du trafic. Les médecins envoient le formulaire prévu à l'autorité cantonale responsable de la circulation routière ou à l'autorité de surveillance des médecins. Seuls les candidats qui connaissent cette procédure sont admis au poste de médecin-conseil. Le Bureau juge donc que les bases légales sont suffisantes.

– Information des autorités sociales

Le Bureau a reçu une demande à propos de l'opportunité pour le Service des solutions transitoires (formation entre l'école obligatoire et la formation professionnelle) de communiquer de son propre chef aux autorités sociales des informations sur des individus. D'après la loi sur l'aide sociale, les informations sont en principe transmises par la personne concernée. Si cela s'avère impossible ou inapproprié, elles peuvent être obtenues auprès des autorités du canton ou des communes. Celles-ci peuvent fournir les informations si elles savent de source sûre que les personnes visées perçoivent l'aide sociale et si les informations sont indispensables pour examiner le droit à des prestations. Il faut vérifier pour chaque cas si ces conditions sont réunies.

– Données personnelles dans le cadre de la prévention des accidents majeurs

La publication sur Internet d'une carte des périmètres de consultation indiquant les noms et les adresses des entreprises pour l'exécution de l'ordonnance fédérale sur les accidents majeurs ne peut pas se faire sans base dans une ordonnance cantonale. Si le droit fédéral ne suffit pas, il convient aussi de noter que la publication ne constitue pas une grave atteinte aux droits fondamentaux de sorte qu'elle peut être réglée par voie d'ordonnance.

7 Législation

7.1 Législation fédérale

privatim a pris position dans le cadre de la procédure de consultation sur la loi fédérale sur les mesures policières de lutte contre le terrorisme (MPT) et sur la loi fédérale sur les précurseurs de substances explosibles (LPREX). Lorsque l'association l'a fait ou a répercuté des prises de position de ses membres, le Bureau se rallie à l'avis exprimé, à moins qu'il y ait lieu de tenir compte de spécificités bernoises.

7.2 Législation cantonale

Le Bureau a pris position sur les actes législatifs suivants (à l'occasion des procédures de consultation et de corapport):

– Révision de la loi sur la protection contre le feu et sur les sapeurs-pompiers (LPFSP)

Sur la base de la proposition du Bureau, l'assurance immobilière est tenue de garantir un droit de blocage au sens de l'article 13 LCPD pour les données enregistrées dans son système.

– Révision de la loi sur le personnel (LPers)

Le Bureau a critiqué la révision de la loi sur le personnel, dont le but est de créer les bases pour le traitement des données personnelles résultant de l'utilisation de l'infrastructure informatique de l'administration (p. ex. téléphone, ordinateurs). Il indique (https://www.jgk.be.ch > Surveillance > Protection des données > Actualité) que la réglementation proposée ne remplit pas les conditions prévues dans la Constitution concernant les atteintes graves aux droits fondamentaux. Il a ainsi déploré que le principe d'interdiction d'enregistrement et d'évaluation qui protège les collaborateurs soit affaibli et non renforcé. Il a demandé que les autorités qui peuvent exceptionnellement avoir accès aux données concernées et les évaluer soient désignées avec suffisamment de précision et que les délais de conservation et de destruction des données soient ajoutés pour chaque but d'évaluation. Par ailleurs, il a fait remarquer qu'une application généralisée de la réglementation aux utilisateurs de l'infrastructure qui ne travaillent pas pour le canton doit être évitée dans la mesure où elle conduirait à un relevé de données de la population qui dépasse largement le cadre légal. Aujourd'hui, les données sur l'utilisation des sites Internet cantonaux ne peuvent de toute manière être analysées que si elles sont anonymes.

– Loi sur les fichiers centralisés de données personnelles (LFDP)

La LFDP doit d'une part remplacer la loi actuelle sur l'harmonisation des registres officiels et d'autre part constituer une base légale pour la création de nouveaux fichiers centraux de données personnelles. Le Bureau a signalé le risque important que présentait la centralisation des fichiers lorsque les données collectées par certaines autorités étaient utilisées pas des autorités différentes à d'autres fins que celles prévues à l'origine. La numérisation permet de plus en plus le recoupement des banques de données ainsi que la consultation et l'évaluation d'un grand nombre de données (et même le profilage). Pour que les citoyens ne deviennent pas plus «transparents» encore pour les autorités, le Bureau a exigé que le traitement notamment des données particulièrement dignes de protection soit suffisamment réglementé dans le détail par la loi. A l'occasion de la procédure de consultation (https://www.jgk.be.ch > Surveillance > Protection des données > Actualité), le Bureau a indiqué les changements souhaitables.

– Ordonnance sur l'exécution judiciaire et instruction de l'OEJ concernant l'effacement et l'archivage des données personnelles et des autres données

Les remarques du Bureau n'ont été que partiellement prises en considération. La Direction de la police et des affaires militaires a estimé que le cadre posé par la loi sur l'exécution judiciaire et la loi sur la protection des données ainsi que la possibilité d'un contrôle par un tribunal étaient suffisants. La durée de conservation des données de surveillance recueillies dans le cadre des arrêts domiciliaires (cf. ch. 5) a été maintenue à trois ans bien que le Bureau l'ait jugée disproportionnée.

– Ordonnance exploratoire sur l'annonce électronique des déménagements (OE eDéménagement)

Le Bureau a constaté que le système prévu ne permet pas de garantir que la personne annonçant un déménagement soit la même que celle qui change de domicile, puisqu'aucune identification formelle n'est mise en place (p. ex. au moyen de la signature électronique SuisseID). Il est ainsi possible qu'une personne usurpe une identité et fasse «déménager» une autre personne. Le cas s'est déjà présenté dans un autre canton. La recommandation du Bureau sur le maintien de l'obligation pour les communes de vérifier l'identité des personnes qui déménagent au moyen de leur acte d'origine n'a pas été prise en considération. Le système électronique doit nécessairement être amélioré au plus tard après la phase exploratoire lorsque le projet sera déployé dans tout le canton. En effet, les données inexactes des registres du contrôle des habitants se retrouveront aussi dans les systèmes subordonnés, tels que GERES et la GCP. Dans l'immédiat, il revient aux communes et à leur autorité de surveillance de la protection des données de faire leur possible pour garantir la qualité des données du registre.

– Ordonnance sur les prestations d'insertion sociale (OPIS)

L'OPIS fournit la base légale à l'accès par une application web aux données GERES, qui sont nécessaires pour l'établissement des bons de garde. Le Bureau a proposé aux législateurs de définir l'accès précisément afin que ce dernier se limite aux données nécessaires.

– Ordonnance sur la procédure de taxation (OPT)

La modification de l'OPT permet aux contribuables de déposer leur déclaration d'impôt en ligne à partir du 1er janvier 2019. Le Bureau demandait que le système électronique soit déployé de telle façon que le dépôt en ligne ne soit possible qu'après une claire identification du contribuable. L'Administration des finances a fourni une description détaillée du processus. L'identification se base, comme pour l'identifiant d'accès à TaxMe-Online, sur l'adresse disponible dans la gestion centrale des personnes (GCP). Les contribuables sont informés des étapes nécessaires à l'identification.

– Loi sur les programmes d'action sociale (LPASoc)

Lors de la procédure de consultation, le Bureau a pris position sur la levée du devoir particulier de discrétion des personnes chargées de l'aide sociale (sauf pour les adultes handicapés) (https://www.jgk.be.ch > Surveillance > Protection des données > Actualité). Il a précisé que l'obligation de garder le secret en matière d'aide sociale est déjà «démantelée» à tel point que les effets d'une restriction du cercle de personnes protégées par cette obligation seraient presque nuls. Une modification indirecte de la loi sur l'aide sociale (LASoc) vient encore vider de son contenu le principe du devoir de discrétion de sorte qu'il convient de se demander dans quelle mesure le secret offre encore une protection qui s'étend au-delà des données personnelles particulièrement dignes de protection.

7.3 Registre des fichiers

De nouveaux fichiers ont été ajoutés au registre cantonal. Pour la remise aux Archives de l'Etat, le Bureau a apporté des améliorations à la base de données et au formulaire.

8 Surveillance et décisions de justice

– BE-GEVER

Les recommandations motivées et les recours concernant BE-GEVER sont détaillés au chiffre 5.1.

– Recours administratif concernant la durée de conservation et la communication des fichiers journaux

Par son recours du 26 juillet, le Bureau attaquait devant la FIN la décision négative rendue par l'OIO à propos du contrôle préalable de la plateforme des services DDI. L'abréviation DDI désigne trois services de base: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) et IP Address Management (IPAM). Ces services sont indispensables aux communications utilisant un protocole Internet. L'utilisation, parfois privée, d'Internet par les collaborateurs du canton génère des fichiers journaux. Le Bureau demandait que, faute de base légale, la durée maximale de conservation de ces fichiers soit fixée à six semaines et qu'un allongement de la durée ne puisse être prévu que pour les données qui pourraient se révéler utiles dans le cadre d'une procédure ouverte. Quant à la communication des fichiers journaux à des tiers en général et pour l'instruction des poursuites pénales en particulier, il convient de ne prévoir pareille possibilité qu'à condition que le droit des services compétents de donner leur accord soit respecté. Des données particulièrement dignes de protection sont aussi traitées lors de l'enregistrement et de l'analyse des données secondaires générées lors de l'utilisation des services DDI, ce qui se traduit régulièrement par une atteinte grave portée au droit fondamental des collaborateurs à la protection de leurs données. Faute de base légale formelle, le traitement des données n'est pas autorisé dans la mesure où il n'est pas indispensable à l'accomplissement d'une tâche légale. Il revient aux autorités où sont générées les données de décider de leur communication à des tiers.

– Jugement du Tribunal administratif du 31 janvier (100.2017.72U)

Le Tribunal administratif n'est pas entré en matière sur le recours du Bureau contre une décision de la Chancellerie d'Etat. Le Bureau était d'avis que le traitement de données personnelles dans le cadre de l'exploitation pilote du nouveau système de gestion électronique des affaires n'était pas conforme au droit de la protection des données en l'absence d'une double authentification ou d'une signature électronique des documents enregistrés. Il avait donc précisé que les collaborateurs devaient continuer de documenter l'activité de l'Etat sur papier. Le tribunal a indiqué dans un premier temps que la sûreté de l'information (confidentialité, disponibilité et intégrité) concernant les données personnelles faisait partie des prérogatives du Bureau raison pour laquelle il pouvait formuler des recommandations à ce sujet. Le tribunal a cependant fait remarquer que le Bureau s'était contenté de demander la documentation sur papier du traitement des données et n'avait pas requis la réparation des failles dans la sécurité du programme; il ne pouvait ainsi pas s'exprimer sur les exigences en matière de sécurité dans le dispositif du jugement. Le tribunal a ajouté que, même si le recours avait été admis, les lacunes n'auraient pas été comblées, de sorte que le Bureau n'avait pas d'intérêt digne de protection à l'annulation de la décision et qu'il convenait de déclarer le recours irrecevable. Le tribunal a néanmoins conclu qu'en prévision

d'autres procédures une analyse des risques devait montrer les mesures garantissant la sécurité qui se révèlent proportionnelles ou pourquoi il n'était pas nécessaire de prévoir des mécanismes de sécurité plus performants. L'analyse doit aussi expliquer pourquoi une seule identification suffit dans le canton de Berne pour accéder au système de gestion électronique des affaires tandis que, dans l'administration fédérale, les directives sur la sécurité informatique requièrent une procédure d'authentification à deux facteurs (c. 4.2).

– Jugement du Tribunal administratif du 6 décembre (100.2017.133U)

Le Tribunal administratif a rejeté le recours du Bureau contre une décision sur opposition de l'Administration des finances. Depuis 2016, les contribuables ne peuvent plus recevoir, d'une part, leurs factures sous la forme électronique sur leur portail d'e-banking et, d'autre part, les décisions et les décisions sur recours relatives à la taxation par courrier postal; le même mode d'envoi s'applique aux deux situations. Le Bureau a contesté cet état de fait car la nouvelle pratique ne respectait pas les exigences en matière de protection des données. Le tribunal a rejeté le recours. Après une analyse détaillée, il a constaté que selon la doctrine dominante et la jurisprudence un consentement général ne doit être considéré comme involontaire que lorsque les préjudices qui peuvent découler d'un refus n'ont aucun rapport avec le traitement des données et les buts fixés ou qu'ils sont disproportionnés (c. 3.7). En résumé, les préjudices (soit la réception des bordereaux d'impôt par pli postal) qu'encourent les contribuables qui ne donnent pas leur accord pour recevoir les décisions par voie électronique sont liés aux modalités d'envoi et sont acceptables. Le consentement général est donc considéré comme un acte volontaire et valable (c. 4.2). Le tribunal indique que, si moins de gens choisissent aujourd'hui de recevoir une e-facture, on ne saurait en déduire que les contribuables ayant opté pour cette solution – et donc pour l'envoi électronique des décisions – n'ont pas pris leur décision librement. Selon lui, la seule conclusion que l'on puisse tout au plus en tirer est que les personnes qui ont (nouvellement) décidé de renoncer à l'e-facture ont tenu compte des inconvénients liés à un envoi postal et les ont considérés comme acceptables (c. 4.3).

– Compétence du Bureau vis-à-vis des offices AI

Un citoyen a demandé des renseignements à l'Office AI du canton de Soleure en se fondant sur la législation cantonale sur la transparence. Il souhaitait connaître le nombre de cas traités par deux médecins parmi les 109 expertises réalisées pour l'AI entre 2012 et 2014 attestant d'une incapacité de travail de plus de 40 pour cent ainsi que, dans ce pourcentage, le nombre de cas qui ont été suivis d'une invalidité justifiant l'octroi de prestations. L'autorité soleuroise a rejeté la demande et a estimé que l'autorité de surveillance de la protection des données impliquée n'était pas compétente. Le tribunal administratif du canton de Soleure, puis le Tribunal fédéral ont reconnu que les offices AI n'étaient pas des organes de la Confédération eu égard à la protection des données, bien qu'ils s'en approchent et qu'ils appliquent le droit fédéral, et n'étaient donc pas soumis à la loi fédérale sur la protection des données. Le législateur fédéral n'a pas souhaité assujettir les offices AI à la loi sur la transparence non plus. L'arrêt rendu par le Tribunal fédéral constate que les offices AI sont soumis au droit du canton qu'ils desservent, raison pour laquelle les autorités de surveillance respectives sont compétentes (arrêt du 27 juin 2018 [1C 461/2017]).

9 Collectivités de droit communal

Dans le cadre de la haute surveillance qu'il exerce, le Bureau conseille les autorités communales de surveillance qui le demandent. L'autorité de surveillance de la commune d'Ostermundigen a notamment demandé l'avis du Bureau pour la transmission de données à iCampus (convention-type), l'organe de surveillance de la paroisse générale catholique romaine de Berne a posé des questions sur la stratégie informatique qu'elle prévoyait de mettre en œuvre et plusieurs autres communes se sont informées au sujet du RGPD (cf. ch. 6).

10 Points abordés dans le rapport précédent

(3: suivi des contrôles préalables effectués en 2017, 5: contrôles préalables effectués, 8: jugements du Tribunal administratif sur les recours de droit administratif relatifs à BE-GEVER et à la notification des ordonnances et décisions de l'Intendance des impôts par voie électronique).

11 Proposition

Il est proposé au Conseil-exécutif et au Grand Conseil de prendre connaissance du présent rapport conformément à l'article 37 de la loi sur la protection des données.

19 mars 2019

Le délégué à la protection des données: *Ueli Buri*