Kanton Bern
Canton de Berne

Rapport d’activité Bureau pour la surveillance de la protection des données 2025

Bureau pour la surveillance de la protection des données Février 2026

Impressum

Édition : Bureau pour la surveillance
de la protection des données du canton
de Berne

Maquette et réalisation : noord.ch
Illustrations: aurelmaerki.ch

1 Avant-propos

« Me voilà rassuré ! » Cette réaction recueillie à l'issue d'un échange avec des secrétaires communales et communaux concernant la nouvelle loi sur la protection des données m'a vraiment fait plaisir. Il n'y a pas de raison d'avoir peur de la protection des données ! Les règles essentielles que prévoit déjà notre Constitution cantonale, et qui sont maintenues, ne sont en fait pas si compliquées si on les explique simple-ment. Le « principe de légalité » signifie qu'une employée ou un employé communal est autorisé à traiter des données si cela est nécessaire pour l'accomplissement de son mandat légal. Si la personne peut justifier pourquoi elle a besoin des données pour son travail, leur traitement est autorisé. Quant au « principe de proportionnalité », il signifie simplement qu'on a le droit de traiter uniquement les données dont on a vraiment besoin (il ne suffit pas que ça facilite le travail) et de les conserver uniquement aussi longtemps qu'on en a besoin.

C'est pareil pour les personnes concernées : elles comprennent bien mieux leurs droits et les limites de leurs droits quand on les leur explique à partir de situations concrètes, par exemple comment il se fait qu'aucun service central ne puisse fournir à quelqu'un une liste complète des données que l'administration traite à son sujet (lire l'article du 4 novembre 2025 sur notre site, rubrique « Actualités »).

C'est pourquoi, dans le cadre de son mandat de conseil à l'intention des autorités et des personnes concernées, le Bureau de la surveillance de la protection des données (ci-après « BPD ») s'attache davantage à proposer des informations adaptées au grand public et à les présenter sous une forme intéressante et accessible. Une fois intégrés le but premier de la protection des données et les quelques principes juridiques applicables, le simple bon sens suffit pour faire correctement une grande partie du travail.

Il en va autrement de la sûreté de l'information. Dans un monde numérique et interconnecté, où ni les données à protéger, ni les risques et les attaques ne sont visibles et tangibles, la simple intuition ne suffit pas. Dans ce contexte, une démarche structurée doit apporter la clarté nécessaire pour pouvoir prendre les bonnes mesures. C'est pourquoi le BPD s'attachera spécialement à expliquer aux communes quels sont les risques associés à la numérisation de leurs traitements de données et comment elles peuvent ramener ces risques à un niveau supportable. Ce qui est en jeu, c'est non seulement la confidentialité des données, mais aussi – et surtout – leur disponibilité. En effet, si une commune est tout à coup empêchée d'accéder à ses données, elle se retrouve dans l'incapacité d'accomplir correctement voire d'accomplir tout court ses tâches les plus élémentaires.

La protection des données n'est donc pas seulement dans l'intérêt des citoyennes et des citoyens ; elle est essentielle pour les autorités communales elles-mêmes. Le BPD doit donc proposer à la fois des informations qui parlent à tout le monde et des conseils professionnels aux autorités. C'est dans cet esprit que nous nous réjouissons de l'entrée en vigueur à venir de la nouvelle loi sur la protection des données et d'une collaboration avec les communes sans appréhension.

Ueli Buri, délégué à la protection des données

2 Le fondement de notre travail

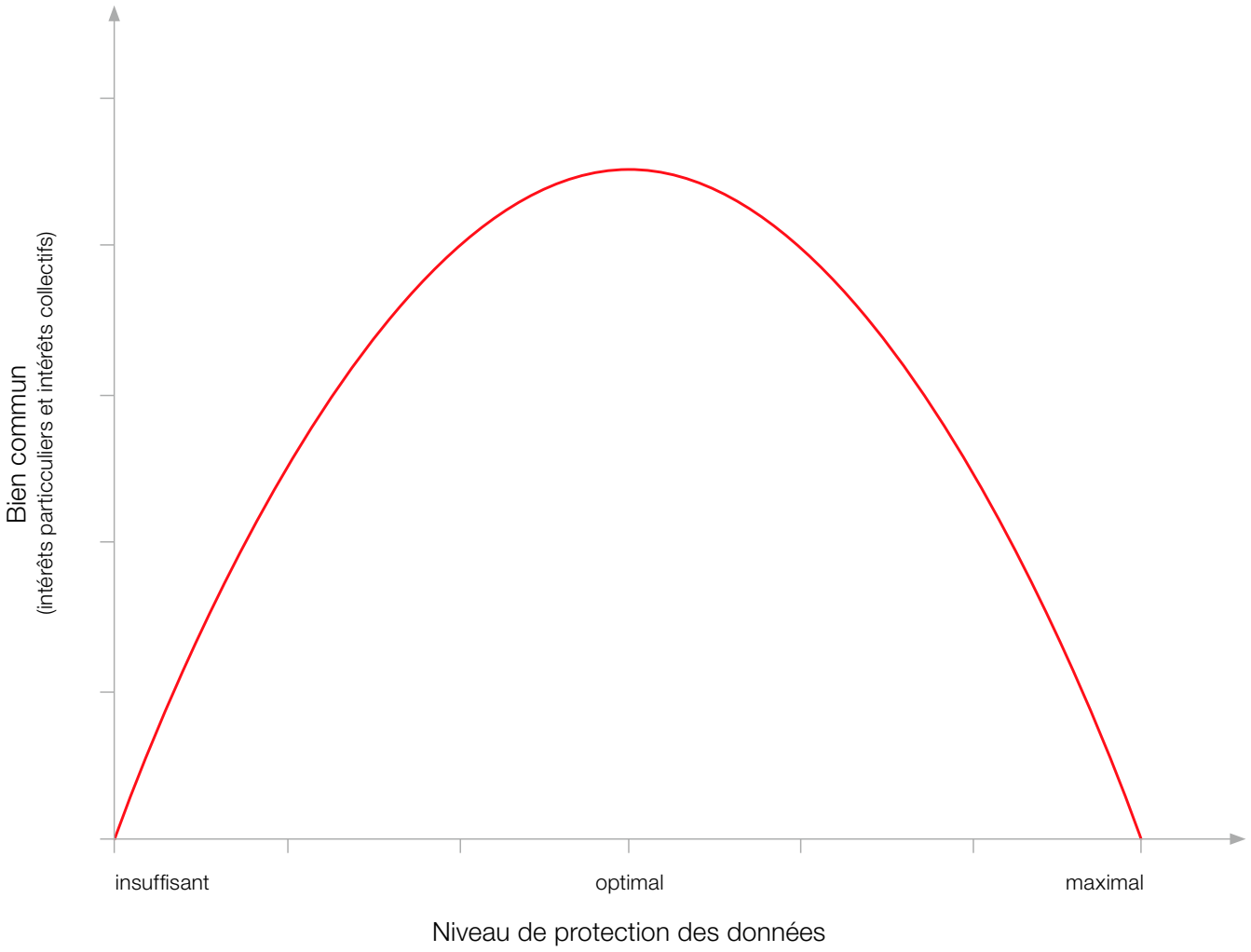
Droit fondamental à la protection des données

La protection des données n'est pas un simple bonus, mais un droit fondamental : voilà ce que l'on a pu entendre au Grand Conseil lorsque la révision de la loi sur la protection des données a été adoptée en première lecture. Et c'est bien de cela qu'il s'agit ! La protection de la sphère privée, qui comprend le droit à l'autodétermination informationnelle (c.-à-d. le droit de chaque personne de pouvoir déterminer si des données la concernant sont traitées ou non et dans quels buts), est un droit fondamental protégé par la Constitution fédérale comme par la Constitution cantonale. Un droit fondamental ne peut faire l'objet d'une restriction qu'à certaines conditions : la restriction doit reposer sur une base légale suffisante, servir un intérêt public prépondérant et être proportionnée au but poursuivi (c.-à-d. être *adaptée* et *nécessaire* et avoir des *conséquences supportables* pour les personnes concernées). Évidemment, ces conditions valent aussi pour le traitement des données personnelles par les autorités. Selon la Constitution cantonale, les autorités doivent par ailleurs s'assurer que les données traitées sont exactes et les protéger contre un emploi abusif (sécurité des données).

Quand un droit fondamental individuel entre en collision avec des intérêts collectifs

Vous l'aurez compris : aucun droit fondamental ne s'applique de manière absolue et sans exception. La même Constitution qui garantit le droit à la sphère privée attribue aux autorités cantonales et communales des tâches à accomplir dans l'intérêt de la collectivité, par exemple dans les domaines de l'éducation, de la formation, de la santé, de l'économie ou de la sécurité. Or, pour pouvoir accomplir ces tâches, les autorités ont besoin de traiter des données personnelles. Le droit individuel à la sphère privée entre donc en collision avec le droit collectif à un bon fonctionnement de la collectivité publique.

C’est pourquoi la protection des données garantie constitutionnellement est considérée comme *adéquate* lorsque le meilleur équilibre possible est atteint entre les intérêts individuels et les intérêts collectifs. Le niveau de protection des données est optimal lorsque le bien commun découlant de la réalisation des intérêts individuels et des intérêts collectifs est maximal, comme l’illustre la courbe ci-dessous.



Trouver la bonne mesure

Si la protection des données est trop faible, des droits fondamentaux individuels sont lésés. Si elle est trop forte, les autorités ne peuvent plus accomplir leurs tâches, ce qui porte atteinte au droit des citoyennes et des citoyens à un bon fonctionnement de la collectivité publique.

Droits et devoirs : la LCPD

La loi cantonale sur la protection des données (LCPD), dans sa version en vigueur comme dans sa version révisée, précise les *devoirs des autorités* lors du traitement de données personnelles. Par autorité, il faut comprendre l'administration, mais aussi les autres entités chargées de tâches publiques, comme les écoles ou encore les hôpitaux. Quant au traitement, il se définit comme toute activité ayant directement trait aux données personnelles, qu'il s'agisse de les recueillir, de les conserver, de les modifier, de les combiner, de les communiquer ou de les détruire. Le recueil de données est autorisé uniquement dans un but déterminé et il est en principe interdit d'utiliser des données à d'autres fins que celles prévues.

La LCPD régit aussi les *droits des personnes concernées*, à savoir le droit aux renseignements et à la consultation de leurs données, à leur rectification si elles sont fausses et à leur suppression lorsqu'elles ne sont pas nécessaires.

Les autorités de surveillance de la protection des données du canton et des communes s'assurent que les autres autorités accomplissent leurs devoirs dans le respect des droits des personnes concernées. Leur statut et leurs devoirs sont également réglés dans la LCPD.

La révision adoptée en décembre dernier ne change rien à ces principes. Elle comble des lacunes existantes, concrétise et améliore la protection des données et donne au BPD davantage de moyens de surveillance. De notre point de vue, la modification centrale apportée par la révision est l'extension de notre domaine de compétence. À l'avenir, nous exercerons notre activité de conseil et de surveillance auprès de 330 communes politiques et de plus de 700 collectivités communales. C'est un défi pour nous, mais aussi une grande chance pour la professionnalisation de la protection des données à tous les échelons.

3 Responsabilité et surveillance

La responsabilité de la protection des données et de la sûreté de l'information incombe à l'autorité elle-même. Toute institution qui traite des données ou les fait traiter par des tiers pour accomplir ses tâches légales doit veiller au respect des dispositions légales. Cela s'applique à tous les traitements de données, qu'ils aient ou non été contrôlés par l'autorité de surveillance compétente.

Les trois échelons de la protection des données

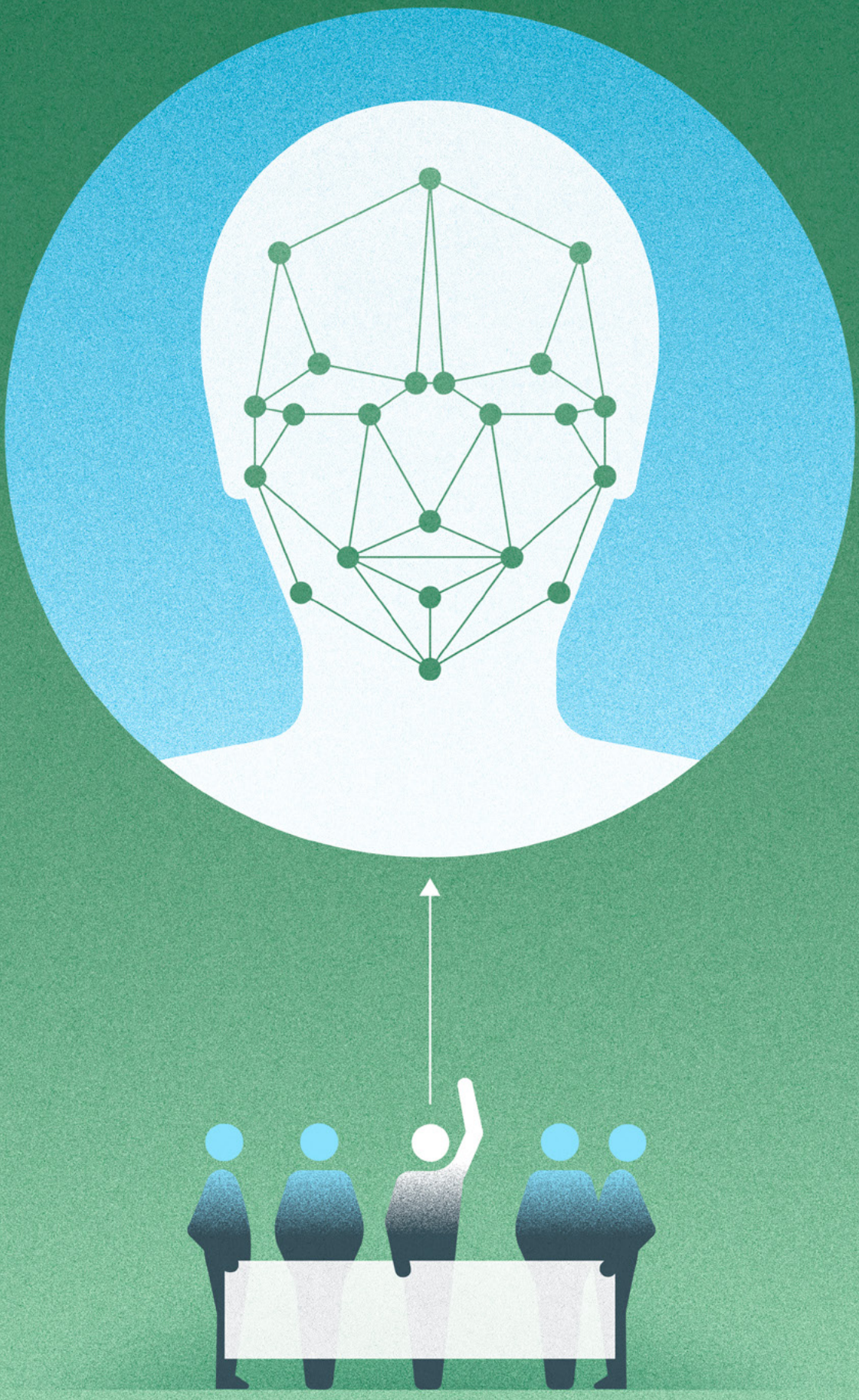
Dans notre pays, le droit de la protection des données présente une structure fédéraliste. Les *autorités fédérales* et les *personnes privées* qui traitent des données sont soumises à la loi fédérale sur la protection des données (LPD) et donc à la surveillance du préposé fédéral à la protection des données et à la transparence (PFPDT). Ainsi, un commerçant de détail qui souhaite placer son entrepôt sous vidéosurveillance doit s'adresser au PFPDT, que la filiale concernée soit implantée à Boltigen, Belprahon ou Berne.

Par contre, les activités des autorités cantonales et communales du canton de Berne sont régies par la LCPD. En l'état actuel, leur surveillance s'inscrit dans la logique du système fédéral : le BPD est compétent pour les *autorités cantonales* tandis que les *communes et les autres collectivités communales* ont chacune leur propre organe de surveillance, lequel est soumis à la haute surveillance du BPD. Avec l'entrée en vigueur de la LCPD révisée (probablement en septembre 2026), l'échelon communal sera supprimé dans la plupart des cas et la surveillance de la protection des données sera centralisée.

Plusieurs échelons dans une même entreprise : l'exemple de l'Hôpital de l'Île

Il n'est pas toujours facile de déterminer de quel échelon relève un traitement de données, d'autant moins lorsqu'une entreprise privée assume des tâches publiques. Prenons l'exemple de l'Hôpital de l'Île. En tant qu'établissement du Groupe de l'Île, il est d'abord assujetti aux prescriptions de la LPD visant les responsables privés de traitements de données et donc soumis à la surveillance du PFPDT. Le BPD n'est donc pas compétent pour les données du personnel hospitalier ou la vidéosurveillance d'un parking qui serait réservé au personnel. Mais lorsque l'Hôpital de l'Île dispense des soins de base, il agit sur mandat du Conseil-exécutif, ce qui en fait une autorité au sens de la LCPD. C'est alors le BPD qui est compétent. Par contre, lorsque l'établissement fournit des prestations surobligatoires, par exemple dans le domaine de la chirurgie esthétique, il agit en qualité d'entreprise privée et, à ce titre, il est assujetti aux règles de la LPD et à la surveillance du PFPDT.

On voit donc que la compétence pour la surveillance de la protection des données de la patientèle est déterminée par la nature et le motif du traitement médical. En ce qui concerne la vidéosurveillance du parking de l'Hôpital de l'Île, le BPD et le PFPDT ont une compétence partagée puisque ce lieu est ouvert à des personnes relevant des deux catégories de soins. En pareil cas, le BPD demande des contrôles préalables et réalise des audits car la protection des droits fondamentaux impose des exigences plus strictes que le droit privé.



4 Notre credo : mieux vaut prévenir que guérir

L’article 34 LCPD énumère les tâches qui incombent au BPD. Le BPD soutient les autorités cantonales dans l’exercice de leur responsabilité en matière de protection et de sécurité des données. Sur le plan informel, il dispense ses conseils aux autorités et, sur le plan formel, il prend position sur les projets d’acte législatif et les autres mesures relevant de la protection des données ainsi que sur les différents traitements de données électroniques prévus qui présentent un risque particulier pour les personnes concernées (contrôles préalables). En outre, il procède à des examens relatifs à la sûreté de l’information dans les systèmes et applications informatiques déjà en service (audits). Le BPD est aussi l’interlocuteur des personnes concernées : il se tient à leur disposition pour fournir des conseils, faire office d’intermédiaire et traiter leurs requêtes. Lorsque la mise en œuvre d’une protection adéquate des données ne peut pas être garantie autrement, le BPD peut rédiger une proposition motivée à l’intention des autorités et recourir jusque devant le Tribunal administratif contre les décisions rejetant une proposition motivée. Cette option ne doit toutefois servir qu’en dernier recours, c’est-à-dire s’il ne faut attendre aucun résultat de la coopération avec les autorités ni des conseils fournis en vue de résoudre les problèmes. La surveillance préventive est un aspect essentiel de notre travail : elle consiste à montrer suffisamment tôt aux autorités où se situent les marges de manœuvre, ce qui améliore l’acceptation. Nous assurons la transparence en tenant le registre des fichiers des autorités cantonales, donnant ainsi aux personnes concernées la possibilité d’exercer leurs droits (renseignement, consultation, rectification et suppression).

5 Nos ressources

5.1 L'équipe

Au 31 décembre 2025, le BPD disposait de 750 pour cent de poste répartis entre neuf personnes. Quatre d'entre elles ont une formation en droit, quatre sont informaticiens ou réviseurs spécialisés en informatique et une est journaliste et rédactrice :

Ueli Buri (délégué à la protection des données) dirige le BPD depuis 2019. À ce titre, il chapeaute la direction stratégique du Bureau ainsi que la définition des objectifs de prestation annuels et gère la conduite du personnel ainsi que les tâches opérationnelles. Par ailleurs, il suit principalement les activités de trois Directions (travaux publics et transports, intérieur et justice [DIJ], sécurité), de la Chancellerie d'État (CHA) et des autorités de justice.

Anders Bennet (délégué à la protection des données suppléant, responsable informatique) est informaticien. Il a travaillé pendant plus de dix ans au service du canton de Berne comme réviseur informatique interne. Il a fait partie de l'équipe du BPD de 2019 au 31 décembre 2025. Sa tâche première consistait à contrôler les systèmes et applications en service (planification et réalisation des audits) ainsi qu'à suivre la mise en œuvre des mesures organisationnelles et techniques dans le domaine de la sûreté de l'information et de la protection des données (SIPD).

Rahel Lutz (déléguée à la protection des données suppléante, responsable juridique) est avocate. Elle travaille pour le Bureau depuis 2009. Elle conseille la Direction de la santé, des affaires sociales et de l'intégration (DSSI) ainsi que de nombreux hôpitaux et autres institutions de santé sur ce qui touche au droit de la protection des données et à l'accomplissement de leurs tâches légales. Elle vérifie les aspects juridiques des documents SIPD lors de contrôles préalables.

Christina Hug Gnägi (collaboratrice scientifique, domaine juridique) est avocate. Elle a rejoint le BPD en avril 2024. Elle suit principalement des dossiers de conseils, de projets législatifs et de contrôles préalables dans le domaine de tâches de la DSSI (administration et institutions de santé) et dans celui de la Direction de l'économie, de l'énergie et de l'environnement (DEEE). En outre, elle conseille et surveille les autorités cantonales dans leurs projets de vidéosurveillance.

Bianca Hüsing (responsable de la communication) a étudié la germanistique et la philosophie avant de se lancer dans le journalisme, où elle a acquis une longue expérience comme rédactrice dans un journal régional bernois. Depuis août 2025, elle s'assure que le Bureau remplit son mandat de conseil et d'information auprès des autorités et du public de manière ciblée, en employant un langage accessible.

Samuel Kaufmann (collaborateur scientifique, domaine informatique) travaille depuis 2016 dans le domaine du développement informatique. Il est entré au BPD en 2023. Il conseille les autorités sur les questions de sécurité informatique et réalise des contrôles préalables sur le plan technique.

Jonas Weber (collaborateur scientifique, domaine informatique) a une formation de spécialiste de la sûreté de l'information et de la cybersécurité. Il est entré au BPD en juillet 2025. Il conseille les autorités dans son domaine d'expertise et réalise des contrôles préalables sur le plan technique.

Michael Weber (collaborateur scientifique, domaine juridique) est avocat. Il travaille pour le BPD depuis 2020. Il traite des demandes de renseignements et de conseils, procède à des contrôles préalables et rédige des prises de position sur des actes législatifs dans les domaines de la Direction des finances (FIN) et de la Direction de l'instruction publique et de la culture (INC), y compris concernant les écoles professionnelles, les écoles moyennes et les hautes écoles.

Urs Wegmüller (collaborateur scientifique, domaine informatique) travaille depuis 2000 dans le domaine de la sûreté de l'information. Il est entré au BPD en 2017. Il conseille les autorités et veille aux aspects techniques des contrôles préalables.

Pour assumer les tâches de conseil et de surveillance en matière de protection des données dans les communes, le Bureau a besoin de quatre postes à plein temps supplémentaires. Lors du débat budgétaire, le Grand Conseil n'en a accepté que 3,2 à moyen terme. Partant du principe que le BPD n'avait besoin d'une ou un spécialiste de la communication que pour expliquer les nouveautés apportées par la révision de la LCPD, il a limité la durée de ce poste à un an. Il n'a pas pris en compte le fait que conseiller 330 communes politiques et plus de 700 autres collectivités de droit communal (en particulier des communes bourgeoises, des paroisses et des syndicats de communes) demandait de passer à une autre échelle. En effet, le BPD va devoir proposer davantage d'offres de soutien et d'information qui répondent aux besoins des communes, lesquels doivent encore être recensés. Ces outils devront être élaborés et tenus à jour. Proposer une communication adaptée aux destinataires sera donc une tâche permanente de l'autorité cantonale de surveillance de la protection des données.

5.2 Les finances

En 2025, les charges du BPD se sont élevées à 1,5 million de francs environ et ses revenus à 30 000 francs. Les charges de personnel constituent son principal poste de dépenses, les autres charges d'exploitation représentant à peine 191 500 francs. Sur ces autres charges, 83,5 % (env. 160 000 fr.) ont été occasionnés par des prestations externes à l'appui de contrôles préalables et de contrôles informatiques. Les revenus du BPD se composent d'honoraires pour des formations continues externes et d'indemnités pour des travaux effectués pour privatim, la Conférence des préposé(e)s suisses à la protection des données.

Le compte de résultats détaillé du BPD, mis en regard du budget et des comptes de l'année précédente, figure dans le rapport de gestion du canton de

Berne que la FIN publie chaque année sur son site Internet (Thème > Finances > Rapport de gestion).

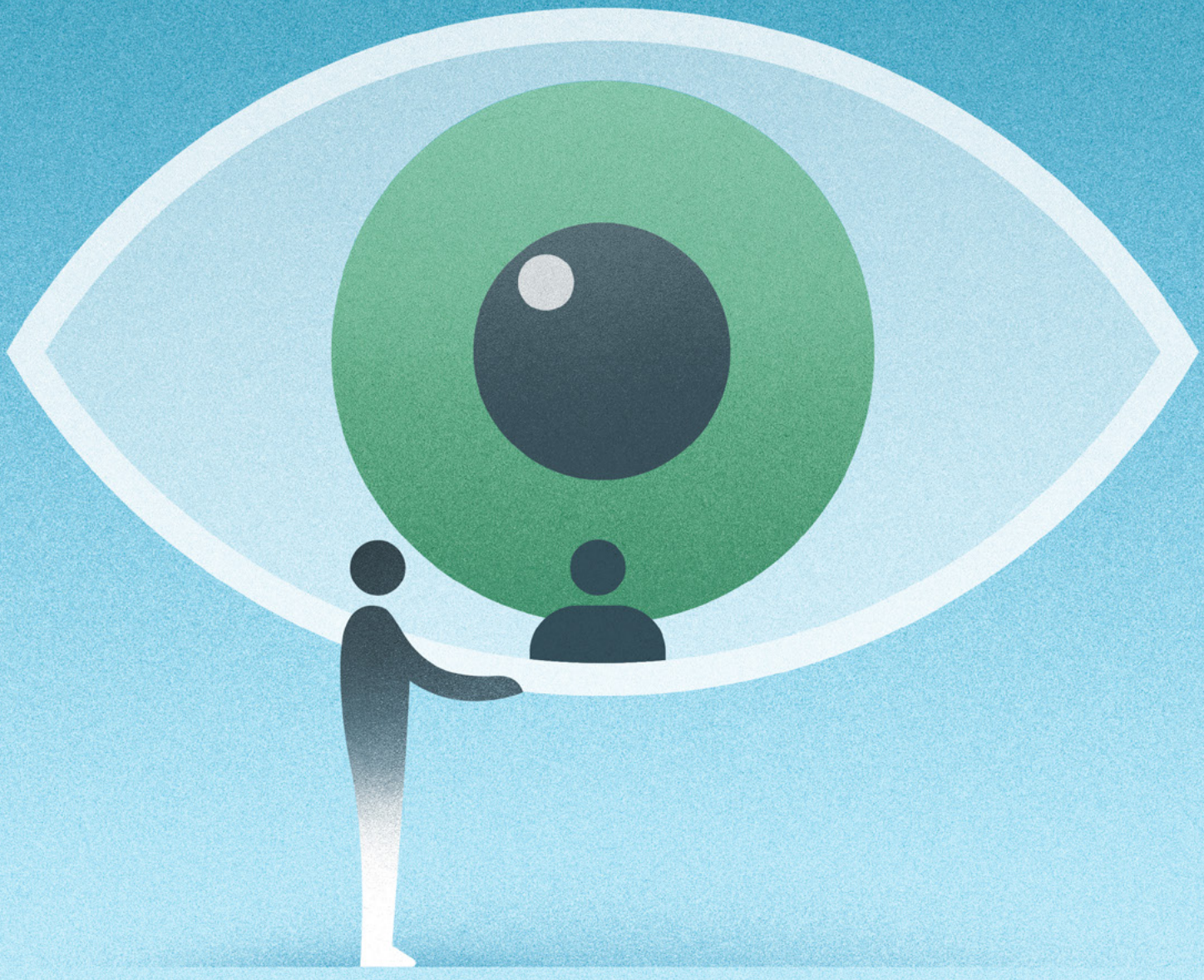
5.3 Le réseau

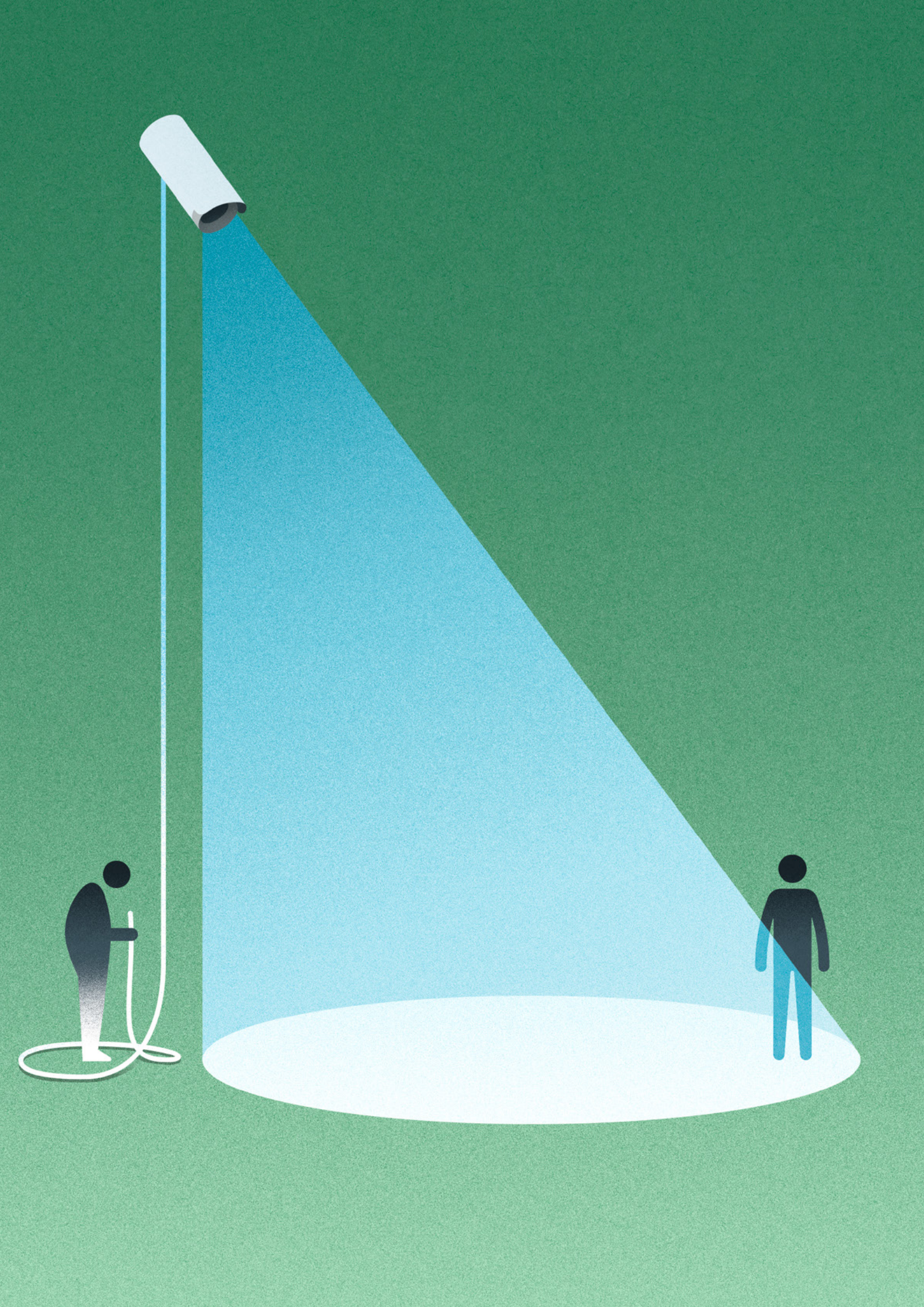
Au sein de l'administration cantonale, le BPD n'est pas le seul organisme qui conseille les autorités dans le domaine SIPD. Les Directions et la CHA disposent chacune d'au moins un organe de contact pour la protection des données, qui conseille leurs offices, et d'une ou un responsable de la sécurité informatique (RSI BE). Les autorités communales peuvent prendre leurs informations auprès de l'Office des affaires communales et de l'organisation du territoire (OACOT) pour les questions de protection des données d'ordre général et auprès des Directions et de la CHA pour les questions particulières (p. ex. concernant la numérisation de l'école obligatoire).

Le BPD s'est donné pour but de développer la prise de conscience et les connaissances de toutes les autorités dans le domaine de la protection des données. C'est pourquoi, cette année encore, nous avons réuni tous les organes de contact. Nous les avons conviés à deux présentations, l'une consacrée au principe de proportionnalité dans la pratique et l'autre à la révision totale de la LCPD. En prévision de l'extension prochaine de notre compétence aux communes, nous avons reçu les services chargés de la surveillance de la protection des données des communes de Berne, Bienne, Köniz et Thoune car ils resteront en fonction après l'entrée en vigueur de la LCPD et nous entendons échanger régulièrement avec eux.

Le BPD accorde par ailleurs une attention spéciale aux contacts institutionnels avec les autorités qui sont régulièrement confrontées à des questions complexes relevant du droit de la protection des données. C'est le cas, par exemple, de l'Office d'informatique et d'organisation (OIO), de la Bedag Informatique SA, de la Police cantonale (POCA), du Groupe de l'Île et d'autres institutions de santé. Dans l'optique d'aboutir à un programme d'audits SIPD coordonné à l'échelle de l'État, nous collaborons en outre régulièrement avec le Contrôle des finances du canton.

En tant que membre de privatim, le BPD est régulièrement en contact avec ses homologues des autres cantons et avec le PFPDT. Ce réseau sert, d'une part, à échanger des connaissances théoriques et pratiques sur les questions qui se posent de la même manière dans tous les cantons. D'autre part, il permet à ses membres de coordonner leur activité de surveillance portant sur des projets qui dépassent les frontières cantonales (p. ex. lorsqu'un groupe hospitalier présent dans de nombreux cantons change de système d'information clinique). Le chef du BPD, Ueli Buri, est membre du comité de privatim et il préside la conférence depuis novembre 2020. Rahel Lutz, déléguée à la protection des données suppléante et responsable juridique, dirige le groupe de travail Santé. Par ailleurs, il y a toujours une personne du BPD qui participe aux autres groupes de travail thématiques (actuellement : cyberadministration, sécurité et TIC). Pour de plus amples informations, voir les sujets traités en 2025 sous le point 6.8 plus bas.





6 Nos activités en 2025 : morceaux choisis

Si nos tâches sont très variées – conseil, formation continue et surveillance sont au menu –, le contenu de notre travail l'est encore plus. Tantôt nous déterminons pour une clinique si elle est en droit de remettre le dossier d'une personne ayant subi une mesure de placement à sa fille, tantôt nous expliquons à une personne détenue pourquoi l'administration pénitentiaire a le droit de lire son courrier. Un jour nous prenons position sur la plateforme de santé cantonale, le jour suivant nous entamons le contrôle préalable d'un nouveau logiciel d'état civil ou nous nous rendons dans un hôpital pour contrôler la sécurité des serveurs.

Nous vous proposons ici une sélection des affaires qui ont occupé le BPD en 2025. Elles concernent tous nos domaines de tâches et ont une portée particulière ou illustrent bien notre travail.

6.1 Conseils à l'intention des autorités

Sécurité des échanges de courriels au Grand Conseil : fastidieux mais indispensable

Le quotidien des membres du Grand Conseil est compliqué. Ils mènent une triple vie (personnelle, professionnelle et politique) et ont donc souvent autant de boîtes de courrier électronique. Afin d'alléger un peu leur charge administrative, ils ont déposé une proposition de renvoi dans le cadre de la révision de la LCPD : ils ont demandé au Conseil-exécutif d'élaborer une disposition leur permettant d'utiliser leur compte privé pour les affaires politiques et d'y faire suivre leurs courriels de service, pour autant que le droit de rang supérieur ne l'interdise pas. Or, le droit de rang supérieur l'interdit. Lors d'une audition devant le Bureau du Grand Conseil, le chef du BPD Ueli Buri a expliqué pourquoi des comptes privés n'offrent pas un environnement sécurisé pour des données personnelles sensibles et des secrets d'État. Un certain nombre de parlementaires utilisent des fournisseurs d'accès tels que GMX, Microsoft (Hotmail) et Google (Gmail), qui peuvent lire leurs échanges de courriels et même en utiliser le contenu à des fins de publicité ou d'entraînement. Même avec les autres fournisseurs d'accès, le risque de lecture par des tiers n'est pas exclu si les messages ne sont pas cryptés. Pour faire court, les personnes qui reçoivent ou transmettent des données sensibles sur leur compte privé ne peuvent pas les protéger d'une utilisation abusive, violant ainsi l'article 18, alinéa 2 de la Constitution cantonale, qui s'applique à la fois aux autorités administratives et aux parlements.

De plus, les membres du Grand Conseil sont soumis au secret de fonction. S'ils diffusent des contenus confidentiels, ne serait-ce qu'à une entité de taille inconnue comme Google, ils commettent donc un acte illicite. Et parce qu'ils

ne peuvent pas savoir à l'avance qui leur enverra quelles informations, il n'est pas admissible non plus de mettre en place un transfert automatique des courriels de service.

Il est clair qu'utiliser plusieurs comptes et appliquer des mesures de sécurité supplémentaires est fastidieux. Mais c'est indispensable pour protéger les citoyennes et les citoyens, dont le Grand Conseil représente au final les intérêts. Ces mesures de sécurité évitent en outre aux parlementaires eux-mêmes de commettre des actes illicites. L'été dernier, on a pu voir dans les médias combien les dangers d'une gestion inappropriée des données pouvaient être concrets. Les données de 44 politiciennes et politiciens fédéraux suisses ont atterri sur le dark net parce que ces personnes avaient utilisé leurs adresses de service à d'autres fins.

Dans ce contexte juridique et factuel clair, la Commission des institutions politiques et des relations extérieures (CIRE) du Grand Conseil a opté pour la recherche d'une solution technique. Par voie de motion, elle demande au Conseil-exécutif de mettre en place une infrastructure informatique plus adaptée à la pratique. Le Grand Conseil devrait examiner cette intervention lors de sa session de printemps.

Ce débat n'a rien changé à la deuxième lecture de la LCPD révisée.

Caméras de surveillance factices

Les caméras de surveillance factices (leurres) sont utiles. Elles coûtent moins cher que les véritables caméras, ne nécessitent pas d'entretien et remplissent malgré tout leur but : dissuader les malfrats de passer à l'action. Comme en plus elles ne filment personne, elles ne sont pas assujetties à la législation sur la protection des données. Est-ce une meilleure option que la vidéosurveillance ?

Pour faire court, non. Même si elle est fictive, une vidéosurveillance peut amener des personnes à changer de comportement et les empêcher de se déplacer librement. Cette pression ne pèse pas seulement sur les délinquantes et les délinquants, mais sur toutes les personnes dans le champ de la caméra-leurre, portant ainsi atteinte à leurs droits. Ce n'est pas pour rien que les dispositifs de vidéosurveillance des autorités sont soumis à des conditions strictes, dont le BPD contrôle le respect. Les caméras-leurres échappent à ce contrôle parce qu'elles ne rentrent pas dans le champ d'application de la loi sur la protection des données. Ce n'est pas la seule raison pour laquelle elles sont illicites. Elles contreviennent aussi au principe de la bonne foi. Ce principe ancré dans les Constitutions cantonale et fédérale veut que les organes de l'État agissent de manière honnête et digne de confiance, ce qui n'est manifestement pas le cas de la simulation.

C’est pourquoi nous avons répondu par la négative à un hôpital qui avait demandé s’il avait le droit de protéger un automate à boissons par une caméra-leurre ou un panneau avertissant que l’endroit est placé sous vidéosurveillance. Le collaborateur de l’institution en charge du projet a eu du nez en nous contactant pour vérifier si ce projet était licite alors qu’au sens strict nous sommes compétents seulement pour les vraies surveillances. Nous avons d’ailleurs fourni des éléments à ce sujet. S’il est établi que les automates subissent des vols, une vidéosurveillance au sens de la loi sur la police serait licite. Dans ce cas, la procédure à suivre serait la suivante : l’hôpital annonce la vidéosurveillance à la POCA et au BPD pour qu’un contrôle préalable soit réalisé et ainsi poser la base d’une mesure antivol proportionnée, conforme aux prescriptions sur la protection des données – et surtout transparente.

Un placement présumé coercitif

Cela fait quelques années que la Suisse accomplit un travail de mémoire sur un sombre chapitre de son histoire : les mesures de contrainte à des fins d’assistance et les placements extrafamiliaux avant 1981. À l’époque, des milliers d’enfants et d’adultes ont été victimes de décisions arbitraires de la part des autorités et de violence institutionnelle. Suite à l’initiative populaire sur la réparation, une loi fédérale entrée en vigueur en 2017 aide les victimes à faire usage de leur droit de savoir et d’obtenir des réparations. Pour savoir ce qui leur est arrivé, elles peuvent demander à consulter les dossiers et documents concernés. Elles sont soutenues dans cette démarche par les archives cantonales. Comme les données en jeu sont par nature des données personnelles particulièrement dignes de protection, la circonspection est de mise, surtout lorsque la demande émane non pas de la victime mais de proches.

Un cas de cet ordre a occupé le BPD au printemps. Une clinique psychiatrique voulait savoir si elle avait le droit d’ouvrir à sa fille le dossier d’un patient présumé avoir été placé de force en 1978 et entretemps décédé. Pour protéger le personnel de la clinique puisque la demande touchait leur secret professionnel, le BPD a recommandé aux Archives de l’État de procéder à une analyse juridique approfondie. Quant à la clinique, il lui a conseillé d’attendre avant de remettre des pièces du dossier médical. Pour réaliser l’analyse juridique recommandée, les Archives de l’État ont interrogé l’Office fédéral de la justice (OFJ). Dans sa réponse, l’OFJ invoque la loi fédérale sur les mesures de coercition à des fins d’assistance et les placements extrafamiliaux antérieurs à 1981. Il confirme que la loi donne aux victimes et à leurs descendants le droit d’accéder aisément et gratuitement aux dossiers des victimes. Les descendants doivent pouvoir vérifier dans un premier temps si leur ascendant a effectivement été placé de force et qui l’a demandé pour quelles raisons. Si la suspicion de placement coercitif est corroborée, l’établissement a le droit de communiquer d’autres dossiers datant de la période où la victime y a séjourné. Le Bureau a alors demandé une précision : peut-on invoquer une loi avant même de savoir si l’on est concerné ? Dans sa

réponse, l'OFJ s'est appuyé notamment sur la jurisprudence du Tribunal fédéral pour recommander d'interpréter la loi en faveur des victimes et donc aussi des victimes *présumées.*

Convaincu par cette argumentation, le Bureau a ensuite demandé l'avis de l'Office de la santé, compétent en matière de secret professionnel médical. Au final, tous les avis obtenus étaient convergents : la fille avait le droit de se renseigner sur le sort de son père.

Instruction religieuse : des règles particulières pour des écoles particulières

En Suisse, l'Église et l'État sont séparés, mais ils collaborent dans de nombreux cas, par exemple pour l'instruction religieuse. Afin d'organiser leur activité dans ce domaine, les paroisses ont notamment besoin des listes des élèves de l'école obligatoire. La communication de ces listes n'est pas un problème au regard du droit de la protection des données. C'est même le contraire puisqu'elle est explicitement prescrite par la loi sur les Églises nationales. Mais qu'en est-il des établissements particuliers de la scolarité obligatoire ? Dans leur cas, la situation juridique est loin d'être claire.

En été 2024, le directeur d'un établissement particulier de la scolarité obligatoire s'est adressé à nous pour clarifier une bonne fois cette question controversée au sein de son établissement. Une paroisse avait demandé un exemplaire de la liste des élèves en invoquant la loi sur les Églises nationales. Par sécurité, l'établissement avait demandé l'appréciation de l'office cantonal compétent, l'Office de l'école obligatoire et du conseil (OECO), qui avait estimé lui aussi qu'il était admissible voire obligatoire de transmettre ces données. Mais la direction de l'établissement n'était pas convaincue. Elle nous a donc demandé si l'obligation de transmettre lesdites données s'appliquait aussi aux données d'enfants et de jeunes vulnérables. Voici ce qu'ont donné nos recherches. Les établissements particuliers ne relevaient pas du tout de la scolarité obligatoire lorsque la base légale régissant la communication des listes d'élèves a été créée. Ils étaient rattachés à l'aide sociale et n'ont été intégrés dans la scolarité obligatoire qu'en 2022. Le passage concerné de la loi sur les Églises nationales n'est donc pas applicable sans autre à ces établissements.

Mais surtout, les données personnelles de leurs élèves sont d'une autre qualité. Le fait de fréquenter un établissement particulier est en soi une information particulièrement digne de protection.

La situation étant insatisfaisante tant pour les écoles que pour les Églises, le Bureau a élaboré une solution de concert avec les Églises nationales catholique et réformée et l'OECO. La solution passe toujours par les représentantes et représentants légaux des enfants et des jeunes. Ces personnes sont informées de l'offre d'instruction religieuse adaptée et, si elles sont intéressées, elles

peuvent prendre l'initiative de contacter les paroisses ou alors elles acceptent d'emblée une communication des données. Cette solution est désormais intégrée dans la foire aux questions concernant l'offre spécialisée de l'école obligatoire et dans les conditions générales contractuelles de l'OECO régissant l'offre des établissements particuliers de la scolarité obligatoire.

Décision « Teams » : l'expression d'une collaboration constructive

M365 offre tout ce dont on peut avoir besoin pour le travail de bureau quotidien : des outils pour écrire, préparer des courriels et des présentations, calculer et téléphoner. Et parce que ces applications peuvent fonctionner sur le nuage (cloud), elles permettent de travailler depuis n'importe où. Mais cette promesse de commodité et de gains d'efficacité n'est pas sans danger : utiliser les services en nuage de M365, c'est abandonner de fait le contrôle de ses données. Il est impossible de déterminer sur lequel de ses serveurs en Europe Microsoft traite les données injectées et qui y a accès.

Malgré des risques connus, M365 connaît un succès croissant, y compris dans les administrations publiques. C'est ainsi que le Conseil-exécutif bernois a décidé, en 2023, d'équiper l'ensemble de l'administration cantonale de la suite M365. Le Bureau a expliqué clairement dès le départ qu'il est illicite de traiter dans le nuage les données sensibles à partir du niveau de protection 2. Le Conseil-exécutif a limité en conséquence l'utilisation de M365. Ainsi, certaines applications comme Word ou Outlook (courrier électronique) de l'administration cantonale sont basées non pas sur le nuage, mais dans le centre de calcul de la Bedag. Pour toutes les applications qui fonctionnent de cette manière, comme OneDrive et SharePoint, une seule et même règle s'applique : les données à partir du niveau de protection 2 sont taboues.

Et pourtant, en bientôt deux ans de pratique, beaucoup d'autorités ont ressenti un besoin croissant d'assouplir cette règle. C'est surtout l'utilisation de Teams pour les échanges téléphoniques quotidiens qui pose problème : faut-il raccrocher dès que la personne à l'autre bout du fil donne des informations sensibles la concernant ? À l'automne dernier, le Conseil-exécutif a ainsi dû prendre une décision sur l'utilisation de M365 pour les données à partir du niveau de protection 2. Avant de se prononcer, il a auditionné le BPD. Notre point de vue n'avait pas changé : autoriser en bloc le traitement de ces données sur le nuage mettrait gravement en danger les droits fondamentaux de citoyennes et des citoyens. Cependant, comme les difficultés rencontrées dans l'administration se rapportaient surtout à Teams, il était envisageable d'assouplir la règle pour cette application, mais seulement pour les conversations téléphoniques et à condition que celles-ci ne soient pas enregistrées. Le Conseil-exécutif a suivi notre recommandation et autorisé la communication de données à partir du niveau de protection 2 dans les conditions indiquées (lire le communiqué du 20 octobre 2025 sur le site du Bureau « Moins de restrictions pour le système de téléphonie ‹Teams› »).

Cet épisode a montré que le gouvernement, l'administration et le BPD travaillent main dans la main. Si l'on regarde ce qui se passe dans d'autres cantons, on constate qu'il ne va pas nécessairement de soi d'écouter l'autorité de protection des données et de suivre ses recommandations. Précieuse au plus haut point, cette relation de confiance repose sur une attitude fondamentalement constructive de la part de toutes les parties.

Protection des données et prévention du cancer dans l'ensemble du canton

En règle générale, les autorités n'ont pas le droit de traiter des données dans un autre but que celui prévu lors de leur collecte et en tous cas dans un but contraire à celui de leur collecte. Autrement dit, si l'administration fiscale se mettait à envoyer à des contribuables des invitations à jouer à des jeux d'argent, elle violerait clairement l'article 5 LCPD. Il n'est pas toujours aussi facile que dans cet exemple absurde d'interpréter le principe de l'affectation à un but déterminé. Dans la réalité, on tombe souvent sur des cas dans lesquels la limite est très floue. En voici un exemple.

Dans le canton de Berne, il existe deux programmes de prévention du cancer du sein : donna et BEJUNE. Le second s'adresse aux femmes vivant dans le Jura bernois ainsi que dans les cantons du Jura et de Neuchâtel. Il participe en outre à un nouveau projet de recherche appelé « BRAICS », dont le but est d'améliorer le taux de dépistage précoce du cancer du col de l'utérus. Pour trouver des participantes entre 50 et 74 ans, l'Association pour le dépistage du cancer BEJUNE souhaite exploiter la banque d'adresses de son programme de prévention du cancer du sein et présenter le projet-pilote BRAICS à 6200 personnes. À cet effet, l'ADC a présenté une demande aux trois cantons concernés, avec copie au délégué à la protection des données du canton de Berne et au préposé à la protection des données et à la transparence Jura Neuchâtel. À la date d'envoi de ces demandes, le projet de recherche dont il est question n'avait pas encore été approuvé par la commission d'éthique compétente. Fort du lien de confiance qui les unit, les deux responsables de la protection des données ont échangé au sujet de la demande de l'ADC. Ils sont arrivés au même résultat : l'utilisation de la banque de données sur laquelle porte la demande ne constitue pas un changement de finalité. Tout d'abord, les deux programmes poursuivent le même but, à savoir prévenir le cancer dans un groupe cible bien défini. Ensuite, l'ADC ne souhaite pas transmettre des données au BRAICS, mais seulement envoyer des invitations à participer au projet. Les autorités de protection des données ont donc donné leur feu vert, pour autant que les ministères cantonaux de la santé partagent cet avis et que la commission d'éthique compétente avalise le projet.

Conclusion n° 1 : il est payant d'impliquer les autorités de protection des données à un stade précoce.

Conclusion n° 2 : la mise en réseau des services chargés de la protection des données dans toute la Suisse au sein de privatim est profitable aussi à petite échelle.

6.2 Conseils à l'intention des personnes concernées

Exécution judiciaire : lecture du courrier

Nos droits fondamentaux sont-ils intangibles ? Pas tout à fait. Pour organiser la vie en société, l'État est obligé de fixer des limites. La privation de liberté en est un exemple flagrant. Une personne condamnée pour un crime perd provisoirement son droit à la liberté, mais pas ses autres droits. Franchir le seuil d'un établissement pénitentiaire ne lui ôte pas sa qualité de sujet de droit. Il lui reste la possibilité de demander à consulter un dossier ou d'agir en vue de protéger ses données, par exemple.

Un détenu incarcéré dans le canton de Berne en est bien conscient. Il s'est déjà adressé plusieurs fois au BPD pour obtenir des renseignements ou des explications juridiques, et dans un cas nous avons pu l'aider à faire valoir un droit. L'an dernier, ce détenu s'est notamment plaint que l'établissement pénitentiaire avait contrôlé son courrier. Il a eu la bonne idée de joindre à son courrier la décision rendue par l'établissement d'exécution judiciaire. Il en ressortait que le contrôle du courrier reposait sur une base légale et que cette base légale était applicable en l'espèce.

Si les personnes incarcérées ont le droit d'entretenir des contacts avec l'extérieur, l'établissement qui les accueille doit néanmoins veiller à ce que cela ne présente aucun risque, que ce soit pour le lieu de détention ou pour le succès de l'exécution judiciaire. Fréquenter les mauvaises personnes pourrait augmenter le risque de récidive. D'après l'établissement pénitentiaire, certaines lettres du détenu portaient des symboles suspects, raison pour laquelle il était nécessaire de les contrôler.

Nous n'avons vu aucune raison de remettre en cause les explications fournies par l'établissement pénitentiaire. Nous avons donc pu répondre au détenu sans l'ombre d'un doute : les droits fondamentaux peuvent être limités lorsque la restriction repose sur une base légale suffisante et répond à un intérêt public. Comme nous venons de le voir, ces conditions étaient remplies. Une restriction doit également être proportionnée, ce qui également le cas ici. En effet, l'établissement pénitentiaire ne contrôle pas toute la correspondance, mais uniquement les courriers faisant

naître un soupçon concret. Elle fait alors une copie de sécurité du courrier concerné, en avertit le détenu et lui rend l'original. Il s'agit à notre avis de la forme la plus précautionneuse de contrôle du courrier que l'on puisse envisager.

Le compteur intelligent en sait-il trop ?

Depuis quelques mois, un nouvel occupant a fait son entrée dans beaucoup de ménages suisses : le compteur intelligent ou Smart Meter. Ce compteur promet une transparence totale sur la consommation d'électricité afin que chaque ménage puisse piloter plus efficacement sa consommation. Il envoie des chiffres au fournisseur d'électricité à intervalles réguliers, chiffres que le ménage consommateur peut consulter.

L'installation du compteur intelligent n'est pas entièrement facultative. Selon la loi fédérale sur l'approvisionnement en électricité, en effet, 80 % des ménages d'une zone de desserte devront en être équipés d'ici la fin 2027. À l'heure actuelle, le taux d'équipement au niveau national dépasse les 50 %. Plus il se répand, plus le compteur intelligent s'attire des critiques. Un citoyen qui s'inquiétait pour le respect de la législation sur la protection des données est allé jusqu'au Tribunal administratif fédéral (TAF), où il a été débouté. Le tribunal a estimé que l'utilisation de compteurs intelligents était conforme au droit et à la protection des données. Selon lui, la nature de la collecte des données et des données elles-mêmes ne permet pas de tirer des conclusions détaillées sur le comportement d'un ménage ou sur les appareils qu'il utilise. De même, les données ne sont pas collectées pour effectuer un profilage, mais pour établir les factures et piloter le réseau. Toujours selon le TAF, le gain d'efficacité recherché répond en outre à un intérêt public.

Le BPD, qui a également travaillé sur la question au cours de l'année sous revue, partage cette vision des choses. En l'espace de quelques semaines, deux citoyens nous ont interrogés à ce sujet. L'un remettait en question la légalité du système dans son ensemble. Il ne voulait pas qu'on collecte des informations sur sa consommation quotidienne ni aucune autre sorte de données. Nous lui avons indiqué l'arrêt du TAF selon lequel la mesure intelligente de données sur la consommation d'électricité est licite, conforme au but de la collecte et proportionnée.

La deuxième demande était dirigée non pas contre le compteur intelligent en tant que tel, mais contre la fréquence des transmissions de données. Le citoyen en question disait avoir lu sur le site de son fournisseur d'énergie que les données de consommation du compteur intelligent étaient lues quatre fois par jour. Il pensait que cette fréquence n'était pas autorisée par l'ordonnance sur l'approvisionnement en électricité. Nous avons donc demandé au fournisseur d'énergie concerné à quoi correspondait la fréquence des transmissions de données. Sa réponse nous a convaincus. Il a expliqué que le compteur intelligent envoyait les données quatre fois par jour non pas à lui, mais à un concentrateur de données. La régularité des transmissions a pour but protéger le système au cas où les données seraient faussées par des intempéries ou autre. Le fournisseur précisait que les

transmissions n'impliquaient actuellement que deux unités techniques, le compteur intelligent et le concentrateur. Pendant les transmissions, les données sont cryptées et pseudonymisées si bien qu'elles ne peuvent pas être rapportées à un ménage. Le fournisseur d'énergie lui-même ne consulte les données qu'une fois par jour, respectant ainsi les prescriptions légales.

Dossiers de police : des caviardages suscitent la méfiance

Avoir le droit de consulter ses propres données est sans aucun doute un droit fondamental. Il est en revanche moins évident de savoir jusqu'où va ce droit de consultation dans les cas concrets. Si les intérêts d'une autorité sont en opposition avec ceux d'une personne privée, une conciliation peut être nécessaire. C'est dans ce rôle que le BPD est intervenu en mai.

Un citoyen condamné pour dommages à la propriété échangeait alors avec la POCA. Comme il soupçonnait des incohérences entre les déclarations des témoins et le procès-verbal d'intervention et qu'il se pensait innocent, il avait demandé à consulter les notes internes de la police sur son cas. Ces notes lui ont été transmises, mais caviardées aux deux tiers. Pour justifier ce procédé, la POCA a invoqué que les passages masqués permettaient de reconstituer sa tactique d'intervention et que leur lecture aurait pu compromettre le travail de police. La lecture de ce document totalement décousu n'a fait qu'alimenter la défiance de base du citoyen. Celui-ci s'est donc adressé au BPD.

Pour pouvoir nous faire une idée de la situation, nous avons demandé à la POCA les documents non censurés (cela ne pose pas de problème dans la mesure où le Bureau est soumis à un devoir de discrétion très strict). Voici quelle a été notre appréciation. Une grande partie des passages caviardés ne présentent pas d'intérêt pour la personne concernée, mais ils sont aussi sans danger. Nous avons donc recommandé à la POCA de limiter le caviardage au strict minimum afin de restaurer la confiance du citoyen, non sans lui adresser nos propositions. La POCA était d'accord, le citoyen s'est déclaré satisfait et une escalade a été évitée à peu de frais.

Consultation de documents : nos possibilités ont des limites

Qui le BPD peut-il aider et de quelle manière ? Dans notre travail quotidien, nous sommes régulièrement confrontés à nos limites. Il arrive souvent que les demandes qui nous parviennent ne soient pas de notre ressort et que nous puissions y répondre tout au plus par des généralités. Dans d'autres cas, nous sommes le bon interlocuteur, mais notre capacité d'action est surestimée. C'est ce qui est arrivé en août 2025. Un citoyen a demandé à consulter le dossier d'une personne sous curatelle résidant en EMS qui lui avait donné une procuration générale. Après avoir demandé l'avis d'une ou un spécialiste, l'Autorité de protection de l'enfant et de l'adulte (APEA) a déclaré que cette procuration

n'était pas valable et a refusé la consultation du dossier. L'APEA a estimé que la personne sous curatelle n'avait pas la capacité de discernement nécessaire pour donner une procuration.

Le bénéficiaire de la procuration n'a pas accepté cette décision et s'est adressé à nous pour dénoncer le procédé. Il nous demandait de reconnaître la procuration et d'obliger l'APEA à lui ouvrir le dossier. Mais cela n'est pas dans nos attributions. Nous avons seulement pu vérifier si l'APEA avait porté atteinte au droit de consultation du citoyen en question. Sur la base des informations en notre possession, nous avons estimé que ce citoyen n'avait pas de droit de consultation et que l'APEA avait agi correctement du point de vue de la protection des données. Nous ne sommes pas en mesure et nous n'avons pas le droit de nous prononcer sur les éléments à la base de cette appréciation, à savoir la décision concernant la capacité de discernement de la personne résidant en EMS et la validité de sa procuration. Nous ne pouvons pas non plus donner d'instructions à une APEA. En pareil cas, nous ne pouvons que conseiller le citoyen et lui indiquer qu'il peut recourir contre la décision, ce qu'il avait de toute façon déjà fait.

Courriers associatifs non sollicités : licites en règle générale

S'il vous est arrivé de déménager, vous connaissez le phénomène : votre boîte à lettres se remplit tout à coup de courriers émanant d'associations ou de partis avec lesquels vous n'aviez eu aucun rapport jusque-là ; ou alors à peine votre enfant vient-il de naître que le voilà invité à rejoindre un groupe de jeux. En général, cela veut dire que votre commune a été sollicitée pour communiquer une liste d'habitantes et d'habitants, avec leurs coordonnées, établie selon des critères déterminés comme l'âge ou le genre.

Mais les citoyennes et les citoyens ne sont pas toujours d'accord avec ce procédé. Durant l'année sous revue, plusieurs personnes concernées ont contacté le BPD à ce sujet, déclarant ne pas avoir consenti à la communication de leurs données. Pour la bonne forme, nous leur avons indiqué que nous n'étions pas – du moins pas encore – compétents pour les collectivités de droit communal. Mais comme nous recevons assez souvent des demandes de ce type, nous prenons la peine d'expliquer aux personnes concernées quelle est la situation juridique générale. Et celle-ci est claire. Les communes ont le droit de communiquer les données de leurs habitantes et habitants à des personnes privées si celles-ci peuvent démontrer de manière vraisemblable que cette communication revêt un intérêt digne de protection. Il peut s'agir par exemple du maintien de la diversité culturelle de la localité. À ce titre, les clubs sportifs, les groupes folkloriques et d'autres organisations sans visées commerciales peuvent obtenir des données d'habitantes et d'habitants. Toutefois, la communication systématique de listes de données doit avoir une base légale dans le règlement communal. La nature des données entre aussi en jeu. La communication des nom, prénom, genre, adresse, état civil, lieu d'origine et dates d'emménagement

et de déménagement est normalement permise, sauf si l'adresse se situe par exemple dans une prison. Les informations sensibles, comme les liens de parenté ou la confession, sont d'emblée exclues.

Tant que la LCPD révisée n'est pas en vigueur, nous ne nous prononçons pas sur la correction de l'action de la commune dans le cas concret. En lieu et place, nous indiquons à la personne concernée quel est l'organe de surveillance compétent dans la commune, en lui précisant qu'elle peut demander, sans avoir à fournir de motif, que ses données ne soient pas communiquées sur des listes.

Une seule personne concernée, mais des intérêts opposés

Aucun droit fondamental ne s'applique de manière absolue. Nous nous en apercevons normalement assez vite, que ce soit lorsque nous décidons de pratiquer la flûte à bec après minuit dans notre immeuble locatif ou de stationner sur une propriété privée. En règle générale, notre liberté s'arrête là où commence celle des autres. Cela semble simple à première vue, mais trouver un juste équilibre entre des droits fondamentaux n'est pas toujours évident dans la pratique. La chose se complique lorsque deux droits appartenant à une seule et même personne entrent en conflit.

Ça n'arrive pas tous les jours, mais en voici un exemple parlant. Début juillet, un citoyen a signalé au BPD une violation potentielle de la protection de ses données. Il expliquait avoir posé à l'OACOT des questions concrètes concernant une procédure de zonage et demandé à consulter le dossier. L'OACOT lui avait répondu que son interlocuteur était la commune tout en transférant son courriel à l'administrateur des constructions de la commune – pour le citoyen concerné, un cas évident de communication de données illicite. Le citoyen estimait que ce transfert de courriel était d'autant plus problématique que l'administrateur en question était partie à une procédure de recours contre un projet de construction dans la même zone. L'OACOT avait-il commis une erreur ? Non, a conclu le BPD après avoir examiné de près les échanges de courriels et les bases légales. Au contraire, l'OACOT *avait l'obligation* de transférer le courriel.

En l'espèce, deux intérêts du citoyen concerné s'opposaient : son droit à l'information et son droit à l'autodétermination informationnelle (= protection des données). Selon la loi cantonale sur l'information et l'aide aux médias, les autorités sont tenues d'informer sur leurs activités d'intérêt public, ce qui est indubitablement le cas de la révision d'un plan de zone, et de donner accès aux documents concernés aux personnes qui en font la demande. En sa qualité d'autorité chargée de délivrer les autorisations, l'OACOT avait examiné et traité ces documents. Mais ceux-ci avaient été établis par la commune, raison pour laquelle c'était à *elle* qu'il incombait d'y donner accès.

Cependant, l'OACOT devait réagir. En effet, en vertu de l'ordonnance sur l'information et l'aide aux médias, l'autorité qui reçoit une demande d'accès à des informations pour lesquelles elle n'est pas compétente doit examiner la demande puis la transmettre immédiatement à l'autorité compétente. La communication par cette voie de données personnelles, à savoir l'adresse électronique de l'expéditrice ou de l'expéditeur, ne porte pas en soi atteinte à la protection des données. Pour qu'il y ait atteinte à la protection des données, il faudrait que des intérêts privés particulièrement dignes de protection s'opposent au transfert du courriel.

L'OACOT avait-il des raisons de penser que des intérêts privés particulièrement dignes de protection de l'auteur de la demande étaient en jeu ? À notre avis, non. Le fait que l'auteur de la demande mentionne une procédure de recours pendante met plutôt en avant son intérêt à consulter le dossier que son intérêt à protéger ses données. L'OACOT aurait-il dû demander la permission de l'auteur avant de transférer son courriel ? Cela supposerait qu'il faudrait en théorie faire de même pour toute demande de cette nature, Or, cela représenterait une charge de travail à notre avis disproportionnée, que l'obligation de transmettre à l'autorité compétente vise précisément à éviter.

6.3 Prises de position formelles

La protection des données est en jeu dans beaucoup de projets de loi, même si le lien ne saute pas toujours aux yeux. Le BPD est donc reconnaissant d'être automatiquement impliqué dans toute procédure de consultation cantonale. Nous avons ainsi la possibilité de nous faire notre propre idée et, au besoin, de prendre position pour indiquer les pièges potentiels à un stade précoce. Nous donnons également notre avis dans le cadre des procédures de corapport internes à l'administration lorsque nous détectons des problèmes ou des ambiguïtés au regard du droit de la protection des données. De même, nous contribuons indirectement aux consultations fédérales lorsque le Conseil-exécutif reprend nos remarques dans ses réponses.

Il nous arrive souvent aussi d'être invités à nous exprimer oralement sur des projets législatifs ou des arrêtés du Conseil-exécutif, par exemple dans le cadre d'auditions.

Un cas d'école : la nouvelle LCPD

Il est rare que nous puissions prendre position sur un projet qui nous concerne directement. La révision de la LCPD a donc été très importante pour nous. Elle concerne le fondement-même de notre activité et elle a des répercussions énormes sur notre travail quotidien (cf. chap. 2). Le résultat des débats

parlementaires a donc été une source de grande satisfaction pour nous. Le projet a été adopté dans sa forme idéale. Le mérite en revient notamment à la CIRE, qui a suivi l'ensemble de nos recommandations et les a défendues avec beaucoup de conviction auprès du Grand Conseil. La commission n'a pas ménagé ses efforts. Elle a examiné avec soin les nombreuses propositions de modification ou de retrait et entendu le BPD à ce sujet. Elle a notamment pris en compte deux souhaits que nous avions présentés fin 2024 (lire le rapport annuel 2024, pt 6.2) et les a fait accepter lors de la première lecture. Avant la deuxième lecture, elle a de nouveau invité le BPD à une audition. Grâce à cela, notre message essentiel a sans aucun doute été entendu : les principes du droit de la protection des données sont ancrés dans la Constitution cantonale et ils restent intacts. La nouvelle LCPD n'est pas plus stricte, mais plus précise que sa version précédente. Il est compréhensible que les communes, en particulier, aient craint un durcissement. La protection des données doit effectivement recevoir plus d'attention. Mais ce n'est pas une conséquence de la révision de la LCPD ; c'est à cause des progrès de la transformation numérique. Ce sont les évolutions ultra-rapides dans le domaine informatique et l'audace des cybercriminels qui obligent à augmenter les exigences en matière de protection.

Quant à notre future compétence dans le domaine communal, nous sommes convaincus qu'elle ne pourra qu'être profitable aux deux parties. Les communes bénéficieront de notre soutien pour honorer des obligations que la LCPD leur impose déjà. En contrepartie, nous connaîtrons les problèmes quotidiens et les besoins des communes et nous aurons encore plus de cas pratiques à traiter dans ce domaine aux multiples facettes qu'est la protection des données, un domaine dans lequel on n'a jamais fini d'apprendre.

Quand des employés de la Confédération assument des tâches cantonales – et inversement

Lorsque vous êtes dans un Intercity en retard, peu vous importe qui contrôle les billets : une employée de la compagnie, un agent cantonal ou une fonctionnaire fédérale. Mais qu'en est-il si cette personne vous demande une pièce d'identité, la photographie et la partage sur un groupe de discussion WhatsApp ? Tout à coup, la question de savoir pour qui travaille la contrôleuse ou le contrôleur n'est plus aussi anodine. Selon la réponse, l'incident relève du PFPDT ou du BPD.

On sait que la police est une tâche souveraine des cantons. Autrement dit, chaque canton est compétent pour la sécurité de sa population. Mais aux postes-frontière et dans les trains longue distance, ce sont souvent des fonctionnaires de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) qui assument les fonctions de protection et de contrôle. Ce dispositif repose sur des conventions de coopération entre la Confédération et les cantons. En 2025, le Bureau a été consulté sur la reconduction de l'accord administratif à cet effet entre la Confédération et le canton de Berne. La première chose que nous avons

remarquée, c'est que le document repose à la fois sur la loi cantonale et sur la loi fédérale sur la protection des données. C'est potentiellement problématique car, en cas de doute, ni le PFPDT ni le BPD ne se sentent compétents. En outre, cela nous a semblé être une erreur. En effet, une tâche cantonale reste cantonale même si elle est assumée par une ou un fonctionnaire fédéral. Et toute personne assumant un mandat du canton est assujettie à la LCPD. Ce n'est qu'après coup que nous avons appris qu'une nouvelle loi fédérale permettra explicitement à l'OFDF d'assumer des tâches de police cantonale et de régler la protection des données dans la convention conclue à cet effet avec le canton. Nous avons donc demandé au PFPDT s'il estimait avoir la compétence de surveillance dans ce domaine. Si sa réponse est positive, les choses seront claires pour nous.

La Confédération et les cantons coopèrent aussi dans le domaine des jeux d'argent. Quand l'exploitant d'un casino est contrôlé de manière trop laxiste ou qu'il met en place des automates non autorisés, cela relève de la Commission fédérale des maisons de jeu (CFMJ). Dans ce domaine, la poursuite pénale est du ressort de l'autorité fédérale, qui peut demander le concours de membres de la police cantonale. Cette forme de « location de services » est également réglée dans une convention. La révision d'une ordonnance afférente présentée durant l'année sous revue prévoyait de donner aux membres de la POCA travaillant pour la CFMJ un accès à la banque de données du personnel cantonal GERES dans l'exercice de cette fonction. Le BPD a rejeté le projet en raison de son caractère illicite. En effet, dès lors qu'un membre du personnel cantonal assume une tâche fédérale, il agit en tant que membre d'une autorité fédérale. À ce titre, il ne peut pas bénéficier d'un accès global à une banque de données que le législateur a explicitement mise en place pour l'accomplissement de tâches cantonales.

Anonymiser ou pseudonymiser ? Un petit détail qui change tout

La politique suisse de la santé est à la veille d'un changement de système radical. Lorsque la loi sur la transplantation révisée entrera en vigueur, c'est le principe du consentement présumé qui s'appliquera. Autrement dit, si vous ne voulez pas donner vos organes, vous devrez exprimer votre refus explicitement. Parce que la mort touche au plus profond de l'existence et de l'intime, la mise en œuvre de cette modification législative demandera la plus grande circonspection, en particulier pour garantir la protection des données. Le BPD a donc étudié de très près les ordonnances afférentes. Dans le cadre de la procédure de corapport, nous avons présenté au Conseil-exécutif de nombreuses propositions de modification et remarques en le priant de bien vouloir les transmettre à la Confédération. L'une de ces remarques concernait la distinction entre anonymisation et pseudonymisation des données. De prime abord, on peut penser qu'il s'agit d'un détail juridique sans importance alors que, dans la pratique, c'est un aspect décisif. Des données *anonymisées* sont définitivement dépersonnalisées. Personne ne peut plus les relier à une personne concrète. Les données *pseudonymisées* sont également dépersonnalisées, mais on peut retrouver les personnes concrètes auxquelles elles se

rapportent au moyen d'une « clé ». On peut prendre l'exemple d'une banque de données dans laquelle les patientes et les patients sont enregistrés non pas avec leurs nom et adresse, mais avec leur numéro AVS. Les numéros AVS sont un identificateur clair, qui ne doit pas être associées à des données anonymisées. Comme les ordonnances relatives à la loi sur la transplantation ne prévoient pas de véritable anonymisation, nous avons proposé de remplacer partout la notion d'anonymisation par celle de pseudonymisation.

Nous avons également proposé quelques corrections concernant les compétences pour le registre des transplantations. La responsabilité de ce registre doit être attribuée à *un seul* acteur, et non pas répartie entre plusieurs autorités. L'avantage est double : la traçabilité de l'action des pouvoirs publics est assurée ; et les citoyennes et citoyens concernés peuvent faire valoir leurs droits auprès de l'autorité compétente.

Le BPD a également proposé de remplacer « nécessaire » par « indispensable » dans toutes les ordonnances (N.B. : dans les versions françaises, « erforderlich » est parfois traduit par « requis » ou par une locution verbale). Nous nous sommes fondés pour cela sur la législation sur la protection des données aux niveaux fédéral et cantonal. Lorsque l'État traite des données personnelles sensibles, il faut que ce soit « impérativement nécessaire » ou « indispensable » à l'accomplissement de ses tâches (il ne suffit pas que ce soit pratique). Autrement dit, il faut en principe qu'il n'y ait pas d'autre solution possible. Cela peut sembler anodin, mais c'est la loi et ce détail peut faire une vraie différence dans les cas d'espèce.

Le Conseil-exécutif a pris en compte les propositions du BPD dans leur ensemble et les a reprises dans sa réponse à la consultation de la Confédération.

Plateforme de santé : une orientation claire, des compétences floues

En septembre, nous avons eu l'occasion de nous prononcer sur un projet de politique de la santé de premier plan : la révision partielle de la loi sur les soins hospitaliers. Tous les hôpitaux répertoriés devront utiliser le même logiciel. Un système d'information clinique remplacera les différentes solutions individuelles et une nouvelle plateforme de santé facilitera la circulation des informations. L'idée est qu'une meilleure interconnexion des hôpitaux améliore l'efficacité de leur collaboration. Ce qui semble logique au premier abord peut parfois être piégeux quand on y regarde de plus près.

L'introduction d'un nouveau logiciel pose nécessairement la question de la protection des données, a fortiori dans le domaine de la santé, où presque toutes les données personnelles sont particulièrement dignes de protection. Une plateforme de santé commune peut améliorer la sécurité de ces données car elle évite d'avoir à se renseigner par téléphone ou par courriel et il est en principe plus facile de protéger *un seul* système que dix systèmes différents. Mais cela

suppose que les conditions soient réunies, à commencer par une distribution claire des rôles. Pour que le BPD puisse vérifier si la plateforme de santé respecte la législation sur la protection des données et offre le niveau de sécurité adéquat, il doit savoir qui l'exploite. La DSSI ? L'Hôpital de l'Île ? En l'état actuel, le projet de loi ne désigne pas clairement l'organisme responsable, comme nous l'avons expliqué dans notre réponse à la consultation (en allemand seulement). Le projet ne précise pas non plus si la plateforme de santé sera une sorte de banque de données ou seulement un outil de transfert.

Ce ne sont pas des détails, mais des questions essentielles. Il faut une description claire des compétences et des fonctions pour pouvoir répondre à d'autres questions concernant la protection des données. Une question se pose en particulier : qui est le fournisseur du logiciel et quelles sont ses possibilités d'accéder aux données des patientes et des patients ? Le projet de collaborer avec le groupe américain Epic est très controversé, comme le montrent plusieurs réponses à la consultation et une intervention déposée au Grand Conseil.

C'est pourquoi le BPD accordera une attention particulière à la suite de la procédure législative.

6.4 Contrôles préalables

Une autorité qui prévoit un nouveau traitement électronique de données peut être tenue de faire appel au BPD. Un traitement de données est nouveau lorsque, par exemple, certains processus sont numérisés, des logiciels existants sont remplacés ou des données sont collectées dans un nouveau but (généralement suite à une modification législative). Ces projets doivent être soumis à un contrôle préalable, pour autant qu'ils concernent un large cercle de personnes et qu'ils présentent des risques élevés. Les risques sont élevés lorsque les données traitées sont particulièrement dignes de protection ou soumises au secret ou lorsque la technologie employée présente des risques (p. ex. recours au nuage ou à des robots d'intelligence artificielle). Les vidéosurveillances elles aussi sont généralement assujetties au contrôle préalable.

Les procédures sont plus ou moins complexes et demandent donc un temps de réalisation variable. Il faut souvent plusieurs passages (itérations) avant de pouvoir porter une appréciation finale sur un projet. Nous vous présentons ci-après cinq dossiers de contrôle préalable intéressants par leur contenu ou par la procédure mise en œuvre.

NFFS : grosse dynamique, grosse intensité

À circonstances exceptionnelles, mesures exceptionnelles : tel pourrait être le mot d'ordre du contrôle préalable du nouveau système de gestion des cas NFFS. Exceptionnel, NFFS l'est tout d'abord par sa portée : le logiciel sera utilisé par 85 autorités regroupant plus de 2000 utilisatrices et utilisateurs. Le but premier est d'harmoniser la gestion des cas dans les services sociaux ; par la suite, les APEA et les services d'insertion professionnelle auront aussi accès au système. En raison de sa portée, le projet implique deux Directions au niveau cantonal (DSSI et DIJ), deux échelons du système fédéral (canton et communes) et deux entreprises IT. Le système NFFS est exceptionnel également en raison de son calendrier : avant qu'il ne soit généralisé, une sélection de services sociaux testent le système durant une phase pilote.

Ces particularités nous ont conduit à déroger à la procédure de contrôle préalable habituelle dans la mesure où la loi nous le permet. À la demande de la DSSI, nous avons avancé le contrôle de la partie du projet qui prépare la migration des données pour la phase pilote. En effet, le transfert des données de l'ancien système dans le nouveau système de gestion des cas requiert une analyse préalable et une conversion dans un format intermédiaire compatible avec NFFS. Nous avons reçu la documentation concernant cette partie du projet en novembre 2024 et concernant les améliorations demandées peu après. Nous avons ainsi pu donner notre feu vert en janvier 2025.

Nous avons ensuite réalisé le contrôle préalable du projet dans son intégralité, toujours sous le signe de la flexibilité. Nous avons mené à bien la première itération malgré l'absence de certains documents importants. Nous avons communiqué sans attendre nos constatations aux responsables du projet, leur permettant ainsi de réaliser les travaux d'amélioration avant la réception de notre premier rapport final. Les deuxième et troisième itérations ont eu lieu dans la même dynamique, dans des délais tout aussi serrés. Avec notre accord, les services sociaux participant au projet pilote ont pu mettre en service le nouveau système avant la clôture officielle de la procédure. Il y avait une condition : les défauts importants devaient d'abord être éliminés. Si la phase pilote a débuté en décembre seulement, c'est pour des raisons internes au projet.

Grâce à cette flexibilité de part et d'autre, il a été possible de faire évoluer le projet en continu, sans devoir le mettre en pause pendant des semaines ou des mois. La procédure a été d'autant plus complexe, imposant d'innombrables concertations et présentant plusieurs ramifications. L'une d'elles concernait le système d'authentification cantonal basé sur la solution fédérale AGOV. La DSSI, le BPD et l'OIO avaient des idées différentes concernant le niveau de sécurité requis. À notre avis, il était indispensable que les collaboratrices et les collaborateurs s'identifient au moyen d'une pièce d'identité dans la mesure où ils avaient affaire à des données personnelles sensibles. Plusieurs semaines se sont écoulées avant que toutes les parties ne trouvent un terrain d'entente. Pour que les services

sociaux participant au projet pilote puissent néanmoins commencer à travailler avec NFFS, nous avons autorisé temporairement un niveau de sécurité inférieur. Nous avons jugé le risque supportable car la phase pilote était de courte durée et seuls deux services sociaux y participaient. Accessoirement, le débat autour d'AGOV a conduit à la décision de généraliser cette norme de sécurité dans tout le canton.

L'un dans l'autre, le système NFFS aura été l'un de nos projets de contrôle préalable les plus intensifs. S'il a pu être mené à bien avec succès et dans un délai aussi court, c'est grâce à la dynamique que nous venons de décrire – et qui n'a été possible que parce que le BPD a été impliqué dès le départ.

Les dernières retouches (liquidation des points en suspens par la DSSI puis nouvel examen par le BPD) sont encore en cours.

Dialogueur : pas de données personnelles = pas de problème

« Cela fait trois ans que je vis en Suisse, mais je conduis toujours avec mon permis de conduire espagnol. Est-ce que je risque des sanctions ? » « Oui, vous risquez des sanctions, parce qu'un permis de conduire étranger doit être échangé contre un permis suisse dans les 12 mois suivant l'entrée en Suisse. » Ce n'est pas une personne qui fournit une explication aussi claire, mais un dialogueur (aussi appelé agent conversationnel). Cet outil a été mis en service cette année par l'Office de la circulation routière et de la navigation (OCRN) pour répondre à toutes sortes de questions. Mais quand on lui demande des renseignements concernant des tiers, par exemple à qui appartient telle plaque d'immatriculation, il refuse de répondre en invoquant la protection des données. Ce n'est là qu'un des multiples dispositifs mis en place par l'OCRN pour des raisons de sécurité. Un autre de ces dispositifs se manifeste dès l'entame de la « conversation ». Avant même que l'on commence à taper, un message nous prie de ne pas rentrer de données liées à des personnes ni d'informations confidentielles. C'est à l'instigation du BPD que ce message a été étendu au dialogueur vocal de l'OCRN.

Les deux dialogueurs (écrit et oral) ont été soumis à un contrôle préalable en 2025 dans le cadre d'un projet global. À première vue, il ne s'agit pas d'un traitement de données au sens décrit en introduction du présent chapitre. Ces outils n'ont pas pour vocation de récolter des données personnelles, mais de répondre à des questions. Mais pour qu'ils ne recueillent pas de données personnelles, il faut avertir clairement les utilisatrices et utilisateurs. Suite à notre recommandation, cet avertissement initialement prévu pour le dialogueur écrit est aussi diffusé avant chaque conversation avec le dialogueur oral.

L'OCRN a également dû apporter une correction concernant les numéros de portable. Les appelantes et appelants qui le souhaitent peuvent recevoir par SMS un résumé de l'entretien accompagné de liens vers des informations complémentaires. À cet effet, l'agent conversationnel doit traiter des numéros de téléphone

mobile pendant un bref laps de temps. Le projet prévoyait que ces données seraient conservées durant 5 jours et sur le nuage, des paramètres à notre avis inutiles et risqués car ils permettaient de relier les entretiens à des personnes. En outre, le transfert des numéros de téléphone sur le nuage aurait supposé que les sous-traitants Microsoft et Google documentent en détail ce traitement de données avant que l'OCRN puis le Bureau aient examiné la documentation. Cela aurait compliqué et allongé la procédure sans nécessité. En concertation avec le fournisseur du logiciel, l'Office a modifié la durée de conservation : les numéros de mobile sont finalement effacés dès que le SMS a été envoyé.

Comme il y avait très peu de défauts à corriger dans le projet d'origine et que l'OCRN a procédé sans délai aux corrections voulues, le contrôle préalable a pu être mené à bien en quelques semaines seulement. Qu'en dit le dialogueur ? « Je suis heureux que le contrôle préalable à ma mise en service ait été achevé rapidement. Néanmoins, j'aimerais rappeler que je suis là avant tout pour répondre à des questions concernant l'Office de la circulation routière et de la navigation du canton de Berne. »

VacMe devient HEMED

L'application VacMe a connu une ascension fulgurante. Développée et contrôlée en pleine crise du COVID-19, elle a été utilisée pour la campagne de vaccination cantonale. Sa « carrière » s'est arrêtée en même temps que la pandémie. Son exploitation active a cessé début 2025. Désormais, elle fait seulement l'objet d'une maintenance hors ligne afin de disposer d'une solution de sauvegarde pour de futures pandémies. Mais la DSSI a vu un plus gros potentiel dans cette solution informatique qu'elle avait fait développer en Suisse et avec laquelle elle avait accumulé une certaine expérience.

Elle a donc décidé de faire développer une plateforme de services médicaux basée sur l'infrastructure de base de VacMe : la plateforme HEMED (HealthCare Engagement and Management Platform). La plateforme associera à l'application de sauvegarde VacMe d'autres applications visant à lutter contre les maladies infectieuses ou permettant d'organiser et de réaliser les examens médicaux en milieu scolaire. Elle comportera en outre une interface avec le dossier de santé électronique.

Le BPD a contrôlé séparément HEMED parce qu'il constitue la structure de base des différentes applications. De ce fait, le contrôle préalable est spécial à deux titres. Premièrement, nous devons déterminer avec la DSSI quels paramètres et fonctions sont communs à HEMED et aux applications afin de ne pas travailler à double par la suite. Le recoupement de ces données est un processus très fastidieux car plusieurs services sont impliqués et les applications ne sont pas encore totalement développées. Deuxièmement, HEMED est une infrastructure technique sans traitement de données de santé. Notre contrôle préalable est donc principalement technique. Autrement dit, nous vérifions si l'infrastructure remplit

les conditions requises pour protéger les données personnelles sensibles qui seront traitées ultérieurement dans les applications spécialisées. Les applications, quant à elles, font l'objet de contrôles préalables séparés portant plus spécialement sur les aspects juridiques : quelles données peuvent être traitées sur quelle base ? comment les droits d'accès sont-ils organisés ? qui assume la responsabilité principale ?

Du fait de sa complexité, ce projet devrait nous occuper pendant encore un bon bout de temps. Nous avons pu achever la première itération de l'examen de la documentation d'HEMED avant le passage à la nouvelle année.

Feu vert à un logiciel d'état civil

De la naissance à la mort en passant par le mariage, toutes les Bernoises et tous les Bernois ont affaire à l'un des sept offices de l'état civil du canton au moins une fois dans leur vie. Tôt ou tard, ils tombent sur l'application spécialisée PendenZA. Ce programme enregistre et traite toutes les procédures en cours jusqu'à leur clôture, c'est-à-dire jusqu'à ce qu'un enfant soit adopté ou qu'une personne porte officiellement son nouveau nom. PendenZA aide entre autres à gérer les rendez-vous et il établit des statistiques. Il permet de trouver par exemple dans quelle localité le nombre de cérémonies est particulièrement élevé ou quelle est la proportion de personnes étrangères dans la procédure de préparation au mariage. Mais comme il est ancien et pas totalement à la hauteur des exigences en matière de cyberadministration, il est prévu de le remplacer par un nouveau logiciel : PendenZA 2.0. La nouvelle application aura un avantage supplémentaire pour la population : elle permettra de réserver des dates et des locaux et de payer les prestations en ligne.

Ce nouveau logiciel impliquant des traitements nouveaux eux aussi et concernant en partie des données sensibles, PendenZA 2.0 devait subir un contrôle préalable. En janvier 2025, l'Office de la population (OPOP) nous a remis la documentation correspondante et nous avons pu donner notre feu vert une bonne demi-année plus tard.

Nous avons d'abord examiné le projet en détail, en nous arrêtant plus spécialement sur deux aspects. D'une part, nous avons noté une faiblesse concernant le cryptage des données sensibles : les documents étaient bien sauvegardés sous une forme cryptée, mais ils apparaissaient sans cryptage dans les fichiers de journalisation (qui retracent les modifications). D'autre part, une question d'organisation nous a interpellés : pourquoi l'ensemble du personnel des sept offices de l'état civil avaient-ils besoin d'avoir accès à tous les dossiers de PendenZA, et donc aussi aux dossiers des autres régions ? La réponse de l'OPOP nous a paru plausible. Pour éviter les réservations multiples (p. ex. par des couples qui veulent absolument se marier à une date déterminée) ou les tentatives d'escroquerie (p. ex. mariages fictifs), les membres du personnel vérifient si des procé-

dures sont en cours ou ont été rejetées dans d'autres offices de l'état civil. En outre, les cas enregistrés dans PendenZA finissent tous dans le Registre de l'état civil national, auquel sont raccordés tous les offices de l'état civil du pays et le personnel de ces offices est de toute façon soumis à l'obligation de garder le secret.

Pour le Bureau, l'affaire était entendue. Premièrement, les autorités ont pu justifier leur démarche de manière vérifiable en se référant à une base légale (le Code civil). Deuxièmement, les risques sont faibles parce PendenZA ne traite que très peu de données personnelles sensibles et que tous les contenus sont de toute façon effacés au bout de trois ans. Dans ce contexte, une limitation des accès selon les régions du canton aurait été disproportionnée. Nous en avons décidé de même au sujet des fichiers de journalisation non cryptés. L'OPOP nous a néanmoins assurés qu'il recherchait une solution avec le fournisseur du logiciel. Bien que cette recherche ait été encore en cours au moment de la procédure de contrôle préalable, nous avons finalement rendu un avis positif après avoir soigneusement évalué le rapport bénéfices-risques.

Avis négatif après une longue procédure, mais tout de même la clé d'une solution ?

Les nuages sont incroyablement pratiques. Contrairement aux disques durs locaux, ils offrent un espace et une sécurité illimités. Même si votre PC est touché par la foudre ou si l'immeuble de votre entreprise brûle, les données restent intactes et elles peuvent être consultées depuis n'importe quel endroit du globe. Mais le plus gros avantage des nuages est aussi leur talon d'Achille. Dès lors qu'on utilise de tels services, on perd le contrôle de ses données. Celles-ci sont stockées sur des serveurs inconnus. Et plus le fournisseur de nuage est actif à l'échelon mondial, moins on peut savoir où les données sont stockées, où elles sont traitées et qui y a accès. La métaphore du nuage est donc pertinente à un deuxième titre : ce qui se passe en arrière-plan est invisible à tous.

Pourtant, outre les personnes privées, un nombre croissant d'autorités utilisent les services en nuage de grands groupes américains comme Microsoft ou Google, s'exposant ainsi à un risque qui prend corps notamment lorsqu'elles commencent à traiter des données personnelles sensibles. Les groupes américains en question ne proposent toujours pas de solution convaincante pour la gestion des données confidentielles et des données particulièrement dignes de protection. Même cryptées, ces données ne sont pas protégées contre un accès par des tiers. Tout d'abord, les fournisseurs conservent eux-mêmes la clé de cryptage principale. Ensuite, la législation américaine (*cloud act*) permet de les contraindre à remettre aux autorités américaines les données de leur clientèle. Bref : ces solutions ne permettent pas aux autorités suisses de contrôler de manière suffisante qui a accès à leurs données.

En l'état actuel des choses, il est donc impossible de traiter des données sensibles de manière conforme à la LCPD si l'on fait appel à des fournisseurs de services en nuage comme Microsoft ou Google. Les risques pour les personnes concernées sont trop élevés.

C'est ce que le BPD rappelle à toute autorité qui souhaite implémenter un système basé sur le nuage proposé par de tels fournisseurs. Des données sensibles peuvent être traitées de cette manière uniquement si elles sont cryptées et si seule l'autorité concernée dispose de la clé.

Un office du domaine de la formation a néanmoins persisté dans cette voie. Fermement convaincu de pouvoir éliminer les risques, il nous a présenté son projet pour contrôle préalable. Onze mois et de multiples échanges de courriels plus tard, le BPD est arrivé au même résultat qu'avant le contrôle. Sur les 58 défauts relevés au départ, certains avaient pu être résolus, mais le problème de fond restait entier : le risque de perte de contrôle par rapport au fournisseur de services en nuage du fait de l'insuffisance de la solution de cryptage. En juin 2025, nous avons présenté un rapport de clôture négatif, une issue insatisfaisante pour les deux parties au regard du temps et de l'énergie investis.

Mais les jeux ne sont peut-être pas encore faits. Un informaticien du BPD a étudié méticuleusement les offres du groupe en question, et il a fini par trouver. Ce fournisseur propose effectivement une solution dans laquelle la clé de décryptage reste intégralement aux mains du client (solution Hold Your Own Key, HYOK). Ainsi, les données restent cryptées même pendant le traitement, c'est-à-dire pendant les échanges entre le processeur et la mémoire de travail. Mais c'est la seule solution HYOK que propose ce groupe et elle entraîne d'importantes complications. Le BPD vérifiera si cette voie est adaptée pour l'autorité du domaine de la formation et pour d'autres institutions publiques.

6.5 Audits

Le Bureau n'intervient pas seulement *avant* l'introduction de nouveaux traitements de données, mais aussi *après*. Tout comme les contrôles préalables et les conseils, la vérification des systèmes informatiques déjà en service fait partie du mandat légal du BPD. Mais pour des raisons de personnel, il n'est pas possible de réaliser un volume équivalent d'audits, qui requièrent de se déplacer dans les locaux de l'autorité auditée. Le collaborateur compétent (il est seul actuellement) choisit les autorités à auditer selon des critères déterminés, surtout axés sur les risques, et réalise jusqu'à dix audits par an, par lui-même ou en recourant à une aide externe.

Sur les huit audits planifiés durant l'année sous revue, seuls deux ont pu être clôturés. Dans le cas de quatre audits, les examens requis ont été réalisés, mais la clôture (entretien avec le service audité et finalisation du rapport) n'aura lieu qu'en 2026. Ces audits figureront donc dans le prochain rapport d'activité. L'audit de la protection de base de l'infrastructure informatique d'un hôpital a été reporté car cette institution est en cours de transformation opérationnelle. Enfin, il a fallu renoncer à un audit pour des raisons de personnel.

Un changement de culture réjouissant

Passer de la théorie à la pratique n'est pas un long fleuve tranquille. Toutes les recommandations que le BPD formule lorsqu'il conseille des autorités ou réalise des contrôles préalables doivent être appliquées dans la mesure du possible. Nous vérifions chaque année si c'est bien le cas en nous rendant dans les locaux d'une sélection d'autorités. Nous réalisons nos audits seuls ou avec un partenaire. Et là, c'est malheureux, mais un constat revient régulièrement : les exigences légales en matière de sûreté de l'information et de protection des données rentrent souvent en conflit avec une réalité contrainte par le manque de personnel, des budgets limités et des délais serrés. Lorsqu'une unité administrative arrive à la limite de ses capacités dans son cœur de métier, la protection des données passe au second plan. Beaucoup d'institutions n'ont pas de vue d'ensemble du domaine SIPD ; il leur manque des concepts clairs et une attribution des rôles bien définie. Les membres de leur personnel compétents en la matière ont rarement accès aux personnes exerçant les fonctions dirigeantes.

Mais les temps changent. La culture d'entreprise évolue, comme nous avons pu l'observer dans les services que nous avons audités. La conscience de l'importance élémentaire de la sûreté de l'information et de la protection des données se développe, le personnel adhère et s'identifie à cette vision. Les hôpitaux audités en 2025 en ont clairement fait la démonstration. L'employé d'un hôpital nous a dit n'avoir jamais vu, en vingt ans au service de l'établissement, une sûreté de l'information et une protection des données d'une telle qualité.

Nous avons observé un engagement comparable à la Haute école pédagogique de langue allemande (PHBern).

PHBern : sur la bonne voie, mais le but n'est pas encore atteint

Pendant notre audit, la PHBern s'est montrée tout à fait coopérative et sincère. Cette institution de formation et de recherche se saisit systématiquement des questions SIPD, un domaine qu'elle s'apprête d'ailleurs à transférer dans des structures dédiées. Le changement de culture amorcé a été illustré par la présence d'un membre de la direction lors de l'audit.

Cependant, les structures SIPD sont encore en construction. Nous avons constaté 23 défauts dans les neuf domaines que nous avons audités, de la gouvernance SIPD à la sécurité physique. Si les rôles dans la gestion des systèmes informatiques ne sont pas clairement attribués, il y a un risque par exemple que personne ne se sente responsable de la mise en œuvre de la sûreté de l'information et de la protection des données. Et s'il n'y a pas de règles claires concernant les droits d'accès, les mauvaises personnes peuvent avoir accès à trop de données.

Pour pouvoir se défendre contre des cyberattaques de plus en plus professionnelles, il est indispensable de réaliser systématiquement des contrôles de sécurité et des tests d'intrusion, un aspect qui reste déficitaire à la PHBern. Ces déficits organisationnels se doublent d'un défaut concernant l'emplacement physique des serveurs.

Ces exemples montrent que la PHBern a bien avancé, mais qu'elle ne touche pas encore au but. Ses ressources ne lui permettent actuellement pas de progresser plus vite, mais l'institution semble avoir un bon état d'esprit. Les responsables se mobilisent pour la sûreté des données et adhèrent au rapport de clôture de l'audit.

6.6 Autres instruments relevant du droit de la surveillance

6.6.1 Incidents signalés dans le domaine de la protection des données

Même avec une infrastructure informatique sûre, il peut arriver que des données soient perdues ou tombent entre les mauvaises mains – par inattention, ignorance ou négligence. L'important, c'est d'identifier ces incidents, d'empêcher au maximum les dommages et d'éviter que les incidents ne se répètent en prenant des mesures de prévention. À l'heure actuelle, le signalement des incidents est obligatoire uniquement dans le domaine du travail de police et de l'exécution judiciaire. La révision totale de la LCPD étend cette obligation à l'ensemble des tâches publiques. Nous recommandons cependant aujourd'hui déjà à toutes les autorités de nous signaler leurs incidents dans le domaine de la protection des données pour que nous puissions coordonner ensemble d'éventuelles mesures. Chaque année, quelques autorités font usage de cette possibilité, montrant ainsi une culture constructive face à l'erreur et une sensibilité prononcée à la protection des données.

Durant l'année sous revue, neuf incidents nous ont été rapportés, dont une attaque par hameçonnage, un problème de tableau Excel, un oubli de documents dans le train et un courrier électronique accidentellement mis en copie à quelqu'un à qui il n'était pas destiné. Dans deux cas, une utilisation inappropriée de ChatGPT était en cause. L'un de ces deux cas est présenté en détail ci-après car il a retenu l'attention des médias et la question de l'IA est appelée à nous occuper de plus en plus.

ChatGPT : le facteur de risque humain

« Quand et comment dois-je rabattre mes orchidées ? » « Évalue mon IRM ! » « Écris-moi une histoire du soir dans laquelle apparaît mon petit-fils ! » Désormais, nous faisons appel à l'IA dans tous les domaines de la vie, que ce soit pour avoir des conseils quotidiens, un avis médical ou une aide à la rédaction de textes. Mais il y a une chose que très peu d'entre nous savent : les données que nous fournissons à l'IA ne restent pas chez nous ; elles atterrissent sur des serveurs inconnus et sont réutilisées à des fins d'entraînement, sauf si nous désactivons cette fonction. Avec un peu de malchance, nos échanges apparemment privés avec l'IA peuvent être retrouvés avec une recherche sur Google, comme l'ont rapporté divers médias en juillet 2025. Nous sommes donc bien avisés de ne pas partager d'informations confidentielles avec un logiciel d'IA. Cela vaut en particulier pour les institutions publiques comme la Haute école spécialisée bernoise (BFH). Elle a fait la une des médias l'an dernier à cause d'une utilisation inappropriée de ChatGPT, ce qui a conduit le BPD à mener l'enquête. Une employée avait utilisé cet outil afin d'établir un certificat de travail pour un collaborateur et, pour cela, elle avait injecté tout un tas de données de la personne concernée : nom et prénom en clair, date de naissance, adresse, diplômes, etc. La démarche était inappropriée non seulement pour les raisons exposées en introduction, mais parce que plusieurs membres du personnel partageaient un même compte privé sur ChatGPT. Ainsi, non seulement des tiers inconnus mais aussi des collègues ont eu accès aux données de la personne concernée.

Lorsque cet incident nous a été signalé, nous avons contacté la BFH pour vérifier les griefs de la personne concernée et demander à l'établissement quelles conséquences il en tirait. Son responsable de la protection des données nous a présenté une série de mesures de prévention et de droit du personnel, allant d'offres de formation et d'information à un avertissement à l'encontre des membres du personnel impliqués en passant par un entretien avec la personne concernée. Nous avons estimé que cet ensemble de mesures était convenable et propre à prévenir autant que possible d'autres incidents de ce type.

La communication de données relatives à une personne par les autorités publique n'est pas anodine. C'est une violation du droit. Et s'il n'est pas possible de prendre des mesures techniques, comme dans le cas de ChatGPT, il faut au minimum limiter le plus possible le facteur de risque humain, en prévoyant une attribution claire des rôles, des instructions de travail et, au bout du compte, des sanctions.

6.6.2 Contrôle de la recherche automatisée de véhicules

Depuis août 2014, la loi cantonale sur la police contient des dispositions détaillées concernant l'enregistrement automatique des plaques d'immatriculation et la comparaison de ces numéros avec des banques de données policières. Même si cette comparaison ne donne rien, les données peuvent être conservées pendant une durée pouvant aller jusqu'à 60 jours et, dans certaines conditions, être utilisées dans des évaluations ultérieures. Lors de la procédure législative, nous avons critiqué cette collecte de données aboutissant à la constitution d'un stock de grande ampleur (cf. rapport d'activité 2022, pt 6.2), mais sans être entendus par le Grand Conseil. Celui-ci a préféré prescrire que le BPD doit contrôler régulièrement le respect des prescriptions légales et publier ses constatations. Nous pouvons pour cela nous appuyer sur le rapport que la responsable de la protection des données de la POCA est tenue d'établir régulièrement. Nous pouvons aussi réaliser nos propres vérifications. La POCA est en outre tenue de publier chaque année un rapport sur l'efficacité de la recherche automatisée de véhicules.

Parce qu'un recours auprès du Tribunal fédéral était pendant, la POCA a renoncé à conserver lesdites données au cours de l'année sous revue. Nous avons donc limité notre contrôle au rapport que nous a présenté la responsable de la protection des données. Selon ce rapport, les enregistrements des 46 appareils fixes ont généré jusqu'à 796 concordances par mois lors de la comparaison automatisée. Si l'on y ajoute les concordances avec les enregistrements des neuf appareils mobiles, ce sont au total 51 757 concordances qui ont été obtenues de janvier à juillet 2025, conduisant à quelque 150 arrestations pour différentes catégories de délits. Rien dans le rapport ne permet de penser que les prescriptions légales n'ont pas été respectées.

6.6.3 Propositions motivées et recours

Si nous constatons des infractions à la législation sur la protection des données ou des lacunes dans la sécurité des données, nous pouvons recommander d'y remédier en présentant une proposition motivée. Si l'autorité responsable ne veut pas donner suite à la proposition ou n'est prête à le faire que partiellement, elle rend une décision, que le BPD peut attaquer devant la Direction compétente ou le Tribunal administratif. Dans la pratique, nous n'utilisons pas la forme de la proposition motivée pour présenter nos recommandations, notamment lorsqu'elles font suite à des questions relevant du droit de la surveillance, à des contrôles préalables ou à des audits, parce que les autorités concernées sont généralement disposées à appliquer spontanément des recommandations fondées sur des bases techniques. Il faudrait qu'une autorité ne suive pas une préconisation importante (visant p. ex. l'élimination d'une irrégularité évidente ou d'un risque élevé) pour que nous recourions à la voie formelle de la proposition motivée.

En 2025, nous n'avons pas présenté de proposition formelle ni formé de recours contre une décision négative d'une autorité responsable.

6.6.4 Haute surveillance des autorités communales et paroissiales de surveillance de la protection des données

En application de la LCPD en vigueur, toutes les communes et autres collectivités de droit communal ainsi que les Églises nationales ont leur propre autorité de surveillance de la protection des données. Le BPD exerce la haute surveillance sur les organes communaux de surveillance de la protection des données, dont il est l'interlocuteur.

Plusieurs de ces organes, souvent les organes de révision des comptes des communes, ont adressé au BPD des questions car ils avaient des doutes. La plupart des questions portaient sur la communication de données personnelles par une autorité communale à des tiers, par exemple lorsque les personnes concernées avaient demandé le blocage de leurs données. À chaque fois, nous avons expliqué que le blocage des données développe des effets uniquement envers des tiers privés, et pas envers d'autres autorités. Les citoyennes et les citoyens ne peuvent pas utiliser ce dispositif pour empêcher les échanges d'informations entre autorités prévus par la loi.

Nous avons reçu beaucoup de demandes de la part d'autorités communales, soit parce qu'elles ne savaient pas qu'elles avaient leur propre organe de surveillance, soit parce que l'organe communal n'avait pas pu les aider. Là encore, les questions portaient en grande partie sur la communication de données bloquées, mais aussi sur la vidéosurveillance ou sur l'utilisation de nouvelles technologies comme les services en nuage et l'IA.

6.7 Sensibilisation, information

Contribution à la formation du personnel communal et paroissial

Le Bildungszentrum für Wirtschaft und Dienstleistung (bwd) propose différentes formations à l'intention du personnel des autorités communales ou paroissiales. Des membres du BPD y enseignent depuis de nombreuses années la matière « Protection des données et sûreté de l'information ». Durant l'année sous revue, le bwd a proposé des cours aboutissant au brevet de « Bernische Gemeindefachfrau/ Bernischer Gemeindefachmann », une formation destinée au personnel

administratif des écoles de langue allemande et un cours sur la protection des données dans les paroisses. Lors des formations continues, nous avons expliqué les principes généraux de la protection des données à l'aide d'exemples concrets tirés du domaine d'activité des participantes et des participants. Ceux-ci ont été invités à poser des questions en lien avec leur travail quotidien. Ces questions ont été discutées et ont reçu une réponse en plénum.

Le délégué à la protection des données a en outre été convié à l'assemblée annuelle des secrétaires de commune de la région de Berne pour faire un exposé sur la protection des données et sur la révision de la LCPD.

Diffusion de connaissances lors d'événements spécifiques

Sur invitation, des représentantes et des représentants du BPD prononcent des exposés lors de congrès et de formations continues. Durant l'année sous revue, ils se sont exprimés sur la protection des données et les technologies linguistiques lors du séminaire des services linguistiques de l'administration cantonale et sur l'utilisation de M365 dans le canton de Berne lors d'une manifestation du forum suisse sur la protection des données (Datenschutz Forum Schweiz). Ils ont également présenté la protection des données en bref lors d'une formation continue interne proposée par l'Office de l'intégration et de l'action sociale.

Actualité et informations sur le site Internet du BPD

Jusqu'ici, le BPD animait son site Internet sporadiquement. C'est en train de changer. La protection des données et la sûreté de l'information sont trop importantes pour rester dans l'ombre. Nous voulons développer nos activités de communication non seulement pour faire suite à la révision de la LCPD, mais aussi pour sensibiliser le public. C'est pourquoi nous recourons au service de diffusion de nouvelles du canton depuis l'automne 2025. Nous faisons régulièrement état de notre travail quotidien. Nous expliquons nos prises de position sur certains projets législatifs, nous annonçons les nouveautés qui nous concernent directement et nous illustrons la grande variété du domaine de la protection des données en présentant des exemples choisis (rubrique « Scène du quotidien »). Nous évitons les références aux textes de loi au profit d'un langage qui parle aussi aux personnes intéressées peu familières du sujet. Il est possible de s'abonner à nos actualités et de les recevoir automatiquement par courriel.

Le site Internet du BPD est en outre appelé à devenir un guichet d'information pour les autorités communales. Nous voulons élaborer à leur intention des aides qui répondent au mieux à leurs besoins, raison pour laquelle nous avons commencé à recenser ces besoins dès la phase préparatoire de la révision de la LCPD. À cet effet, nous avons eu des échanges avec l'Association des

communes bernoises, deux préfètes et l'OACOT et nous avons participé à une rencontre des secrétaires communales et communaux.

6.8 Coopération intercantonale

Présidence et comité de privatim

Le chef du BPD, Ueli Buri, préside privatim, la Conférence des préposé(e)s suisses à la protection des données, depuis la fin 2020. Privatim regroupe toutes les autorités cantonales et quelques autorités communales chargées de la protection des données, le PFPDT avec voix consultative et la déléguée à la protection des données de la Principauté du Liechtenstein avec le statut d'observatrice. Son but est de faire comprendre les enjeux de la protection des données et de favoriser la coopération entre les autorités chargées de ce domaine. Durant l'année sous revue, la conférence a tenu deux assemblées générales et s'est intéressée principalement au traitement des données de santé et d'autres données sensibles dans des services en nuage. En novembre, privatim a adopté une résolution déclarant que ces données ne doivent pas être traitées avec des logiciels « Software-as-a-Service » (SaaS) proposés par des fournisseurs internationaux (comme M365). Cette résolution a suscité un vif intérêt dans les médias spécialisés et les médias généraux en Suisse. Elle n'est pas non plus passée inaperçue en Allemagne.

Privatim a rédigé 13 prises de position en réponse à des consultations de la Confédération et de conférences intercantonales. Elle en a mis certaines à la disposition de ses membres comme modèle de réponse. La conférence a eu de nombreux échanges avec des organisations ayant une activité intercantonale, notamment Administration numérique suisse, l'agence Educa, la Conférence suisse des offices de la formation professionnelle, la corporation Technique et informatique policières et la Conférence des directrices et directeurs d'Archives suisses. Elle leur a dispensé des conseils sur des questions de protection des données et de sûreté de l'information. Des échanges réguliers avec le PFPDT ont permis de discuter et de clarifier des questions portant sur des détails techniques ou sur la délimitation des compétences de surveillance entre l'échelon fédéral et l'échelon cantonal.

Groupes de travail de privatim

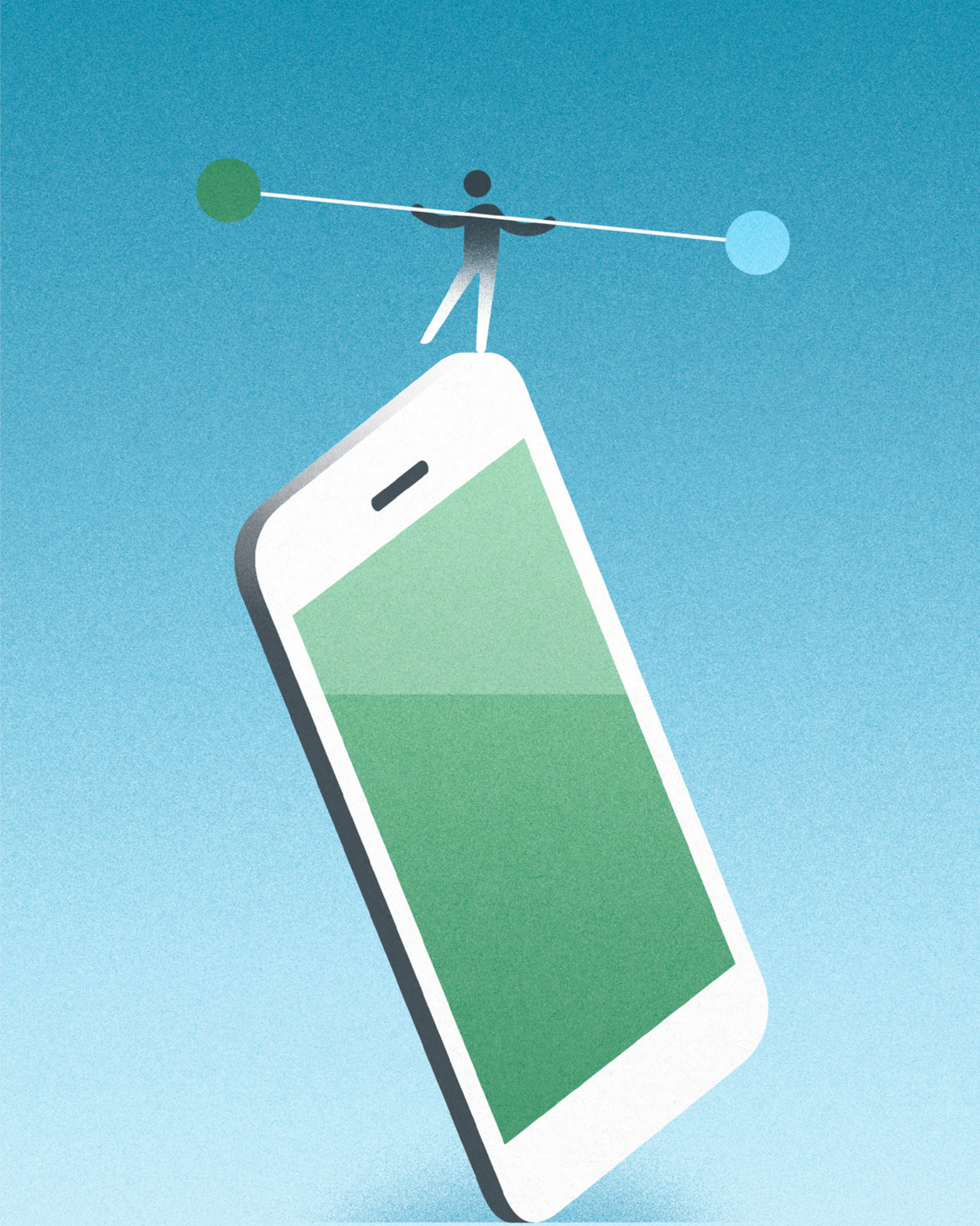
Durant l'année sous revue, le *groupe de travail Cyberadministration* a travaillé sur un aide-mémoire concernant l'utilisation de services basés sur le web pour

produire des textes, des images, des vidéos, des musiques ou des codes et la conformité avec la protection des données. Cet aide-mémoire destiné aux responsables de l'administration cantonale et des administrations communales expose les risques que le nuage présente pour la protection des données et des mesures possibles pour y faire face.

Dirigé par la déléguée à la protection des données suppléante Rahel Lutz, le *groupe de travail Santé* a travaillé notamment sur le chevauchement des compétences de surveillance des autorités cantonales et du PFPDT dans les hôpitaux de droit privé remplissant un mandat public d'approvisionnement en soins (lire aussi au chap. 3 « Plusieurs échelons dans une même entreprise »). Le groupe a en outre eu des échanges théoriques et pratiques à propos de sujets d'actualité concernant tout ou partie des membres de privatim.

Le *groupe de travail Sécurité* a continué de suivre le projet de la Confédération et des cantons visant à mettre en place une plateforme nationale de recherche de données policières (POLAP). Ce projet requiert de nouvelles bases légales, les cantons réglant leurs droits et leurs devoirs par la voie d'un concordat. Manifestement, il y a des cantons qui préfèrent compléter leur loi sur la police plutôt que d'adhérer à un concordat. Cette démarche est de nature à entraîner des difficultés juridiques et pratiques, ce que le Tribunal fédéral a corroboré dans un arrêt relatif à la loi sur la police du canton de Lucerne.

Les organes de surveillance qui ont leurs propres spécialistes de la sûreté de l'information et de la cybersécurité les ont délégués pour discuter, au sein du *groupe de travail TIC*, de questions d'actualité et d'évolutions à caractère technique.



7 Cinq ans d'activité du BPD en chiffres

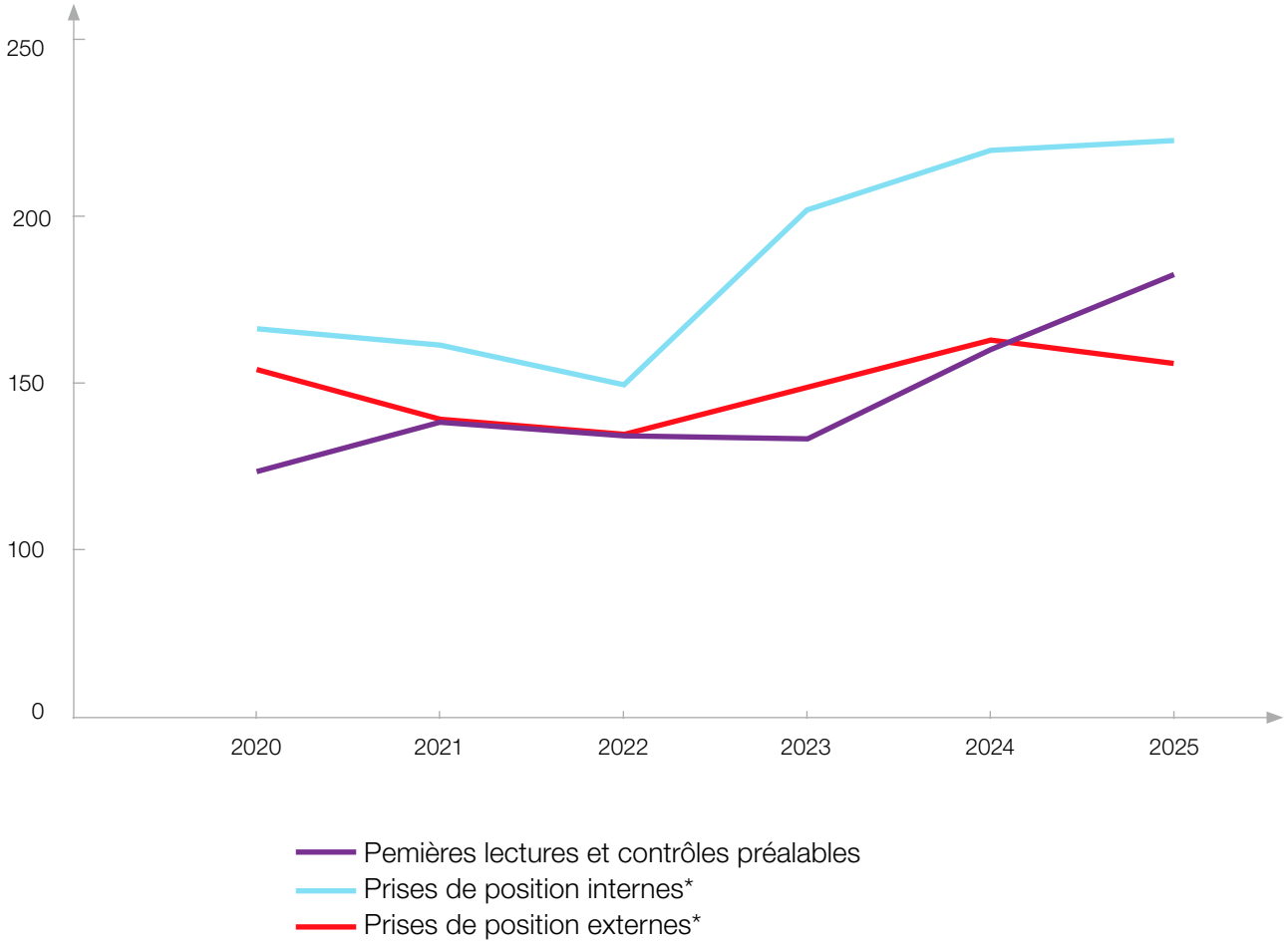
Les morceaux choisis que nous vous avons servis dans le chapitre 6 illustrent notre travail quotidien. Ils montrent les détails auxquels nous prêtons attention dans les contrôles préalables, le type de questions qu'on nous adresse, comment nous trouvons un juste milieu entre excès de rigueur et laxisme. Ce qui manque, ce sont des chiffres.

Le tableau ci-dessous indique combien de dossiers nous avons traités ces cinq dernières années dans nos activités de contrôle préalable, d'audit et de prise de position interne ou externe. Quelques précisions s'imposent. Avant de lancer un contrôle préalable, nous réalisons en général une première lecture. Nous pouvons ainsi déterminer si un projet doit ou non être contrôlé et si la documentation a atteint un stade permettant ce contrôle (c.-à-d. si elle est conforme aux exigences formelles et suffisamment probante). Voici quelques précisions importantes pour bien comprendre le tableau. Tous les contrôles préalables ne sont pas menés à bien l'année de leur ouverture. Certains nous occupent durant plusieurs années ; d'autres peuvent être réglés beaucoup plus vite. Il arrive donc que le nombre de dossiers ouverts et le nombre de dossiers liquidés ne concordent pas et que le nombre de dossiers traités *ne corresponde pas* au total de ces deux rubriques.

	2020	2021	2022	2023	2024	2025
Premières lectures et contrôles préalables:						
dossiers traités	123	138	134	133	160	183
nouveaux dossiers	74	78	69	83	86	88
dossiers clôturés	58	77	94	63	90	95
Audits (y c. audits de suivi)	7	9	12	9	8	2
Prises de position internes*	166	161	149	202	220	223
dont conseils informels	92	80	88	135	146	144
dont prises de position formelles	74	81	61	67	74	79
Prises de position externes*	154	139	134	148	163	156
dont personnes privées	114	98	90	94	105	113
dont autorités communales	40	41	44	54	58	43

* Affaires nouvelles (les chiffres indiqués n'incluent pas le traitement des dossiers ouverts les années précédentes, les prises de position multiples dans un même dossier ni les renseignements téléphoniques.)

Le diagramme à lignes qui suit montre comment le nombre de dossiers qui nous sont confiés a évolué ces dernières années (elle n'inclut pas les audits, que nous planifions de notre propre initiative). On observe une tendance à la hausse, surtout en ce qui concerne les prises de position internes (p. ex. conseils aux autorités et corapports). Le nombre de contrôles préalables a lui aussi nettement progressé ces deux dernières années. Dans le contexte de la révision de la LCPD, nous tablons sur une nouvelle augmentation de nos activités.



8 Proposition

Prise de connaissance

9 Liste des abréviations, glossaire

Liste des abréviations	Glossaire
BEJUNE	(Association pour le dépistage du cancer) Berne, Jura et Neuchâtel
AGOV	Service d'authentification des autorités suisses (identifiant pour les services publics)
APEA	Autorité de protection de l'enfant et de l'adulte
AVS	Assurance-vieillesse et survivants
BFH	Haute école spécialisée bernoise
BPD	Bureau pour la surveillance de la protection des données du canton de Berne
BRAICS	Breast cancer-Related Approach for Increasing cervical Cancer Screening
bwd	Bildungszentrum für Wirtschaft und Dienstleistung (centre de formation professionnelle économie et services)
cf.	Confer
CFJM	Commission fédérale des maisons de jeu
CHA	Chancellerie d'État
ChatGPT	Chatbot Generative Pre-trained Transformer
CIRE	Commission des institutions politiques et des relations extérieures
DEEE	Direction de l'économie, de l'énergie et de l'environnement
DIJ	Direction de l'intérieur et de la justice
DSSI	Direction de la santé, des affaires sociales et de l'intégration
Educa	Agence spécialisée chargée du numérique dans l'espace suisse de formation
FAQ	Foire aux questions (compilation de questions fréquentes accompagnées des réponses)
FIN	Direction des finances
GERES	Système des registres communaux

HEMED	HealthCare Engagement and Management Platform
HYOK	Hold Your Own Key (procédure de cryptage avec autoadministration de la clé)
IA	Intelligence artificielle
ICE	Intercity-Express
IT	Informatique
LCPD	Loi cantonale sur la protection des données
LPD	Loi fédérale sur la protection des données
M365	Microsoft 365
NFFS	Nouveau système de gestion des cas (Neues Fallführungssystem)/r
OACOT	Office des affaires communales et de l'organisation du territoire
OCRN	Office de la circulation routière et de la navigation
OECO	Office de l'enseignement obligatoire et du conseil
OFDF	Office fédéral de la douane et de la sécurité des frontières
OFJ	Office fédéral de la justice
OIO	Office d'informatique et d'organisation
OPOP	Office de la population
PC	Ordinateur personnel
PFPDT	Préposé fédéral à la protection des données et à la transparence
PHBern	Haute école pédagogique de langue allemande
POCA	Police cantonale
POLAP	Plateforme nationale de recherche de données policières
privatim	Conférence des préposé(e)s suisses à la protection des données
pt	Point

RSI BE	Responsable de la sécurité de l'information
SaaS	Software-as-a-Service
SIPD	Sûreté de l'information et protection des données
SMS	Short Message Service
TIC	Technologies de l'information et de la communication
TIP	Corporation Technique et informatique policières Suisse
USA	États-Unis (d'Amérique)

Bureau pour la surveillance
de la protection des données
du canton de Berne

Poststrasse 25
3072 Ostermundigen
+41 31 633 74 10
protectiondesdonnees@be.ch

www.be.ch/bpd