# EXPOSE DES MOTIFS ET PROJETS DE LOIS

- **sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal**
- **modifiant la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD)**
- **modifiant la loi du 1er décembre 1980 sur les dossiers de police judiciaire (LDPJu)**

## 1. Commentaire général

Le 27 avril 2016, l'Union européenne a adopté une réforme de sa législation sur la protection des données. A cette occasion a été adoptée la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ("directive (UE) 2016/680" ou "directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins pénales"). Celle-ci est considérée comme un développement de l'acquis de Schengen.

Lors de ses délibérations sur la révision de la loi fédérale sur la protection des données (LPD), le Parlement a décidé de scinder la révision totale de la LPD en deux volets et de ne traiter dans un premier temps que les modifications législatives indispensables à l'intégration de l'acquis de Schengen. La loi fédérale du 28 septembre 2018 sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS) est entrée en vigueur le 1er mars 2019. Elle a notamment pour objet de mettre en œuvre les exigences de la directive (UE) 2016/680, conformément aux engagements pris par la Suisse dans le cadre de l'accord d'association à Schengen. Elle met en outre en œuvre les recommandations faites par l'Union européenne lors de l'évaluation de la Suisse dans le cadre de l'accord d'association à Schengen. Une fois la révision totale de la LPD en vigueur, il est prévu d'abroger la LPDS au motif que ses dispositions feront double emploi avec celles de la future LPD. La LPDS est ainsi une loi de transition. La LPDS ne s'applique pas aux autorités cantonales. La nouvelle LPD a été adoptée par les chambres fédérales le 25 septembre 2020. Son entrée en vigueur est prévue au 1er septembre 2023.

La reprise de la directive (UE) 2016/680 lie également les cantons. Les dispositions de cet acte doivent être transposées, si besoin est, conformément à la répartition constitutionnelle des compétences prévues en droit interne.

De ce fait, les modifications à intégrer dans le droit vaudois sont les suivantes, avec référence aux dispositions équivalentes de la LPDS :
- Données sensibles: ajout des données génétiques et biométriques (art. 3 al. 1 lit. a ch. 3 et 4 LPDS)
- Notion de profilage (art. 3 al. 1 lit. b LPDS)
- Notion de décision individuelle automatisée (art. 3 al. 1 lit. d et art. 11 LPDS)
- Privacy by default et by design (art. 5 LPDS)
- Registre des activités de traitement (art. 12 LPDS)
- Analyse d'impact et consultation du Préposé (art. 13-14 LPDS)
- Annonce des violations de la protection des données (art. 15 LPDS)
- Conseiller à la protection des données (art. 16 LPDS)
- Larges pouvoirs d'enquête d'office ou sur plainte du Préposé (art. 22-23 LPDS)
- Mesures administratives (art. 24 LPDS)
- Assistance administrative internationale (art. 26 LPDS)

A l'instar du choix opéré par la Confédération, pour tenir compte du fait que, dans le Canton de Vaud aussi, les bases légales générales de la protection des données sont actuellement en évolution, il est proposé de créer une loi spéciale se référant à la LPDS fédérale et consacrée à la protection des données dans le cadre des accords de Schengen ("loi [vaudoise] sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal" – "LPrDS").

La directive (UE) 2016/680 concerne toutes les autorités pénales, tandis que la loi 1er décembre 1980 sur les dossiers de police judiciaire (LDPJu), par exemple, ne concerne que la police. Cependant, la LDPJu doit aussi être elle-même modifiée sur certains points, pour y intégrer diverses exigences des accords de Schengen et du droit supérieur.

Quant à la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD), elle présente des enjeux plus étendus, ne se limitant pas aux accords de Schengen. Une révision générale de cette loi est quoi qu'il en soit prévue. En attendant, il est seulement proposé ici de supprimer une réserve figurant à l'actuel article 3 alinéa 3 lettre c, dont la formulation actuelle est trop exclusive (voir ci-dessous).

Introduire un chapitre concernant Schengen dans l'une des lois cantonales citées exposerait sans doute ces lois à devoir être, de ce fait, fréquemment modifiées en raison de l'évolution de l'acquis de Schengen.

Dans l'immédiat, il s'agit pour le Canton de Vaud, prioritairement, d'être le plus rapidement possible conforme aux exigences des accords de Schengen, puis d'assurer spécifiquement le suivi des évaluations régulières liées à ces accords.

C'est pourquoi les aspects relatifs à Schengen font l'objet d'une loi spéciale, solution par ailleurs adoptée dans l'immédiat aussi au niveau fédéral avec la LPDS. Il convient cependant de relever que cette loi cantonale ne reprend pas tous les éléments de la LPDS en intégralité, dans la mesure où la législation fédérale a un champ d'application plus étendu, intégrant d'autres directives européennes et régissant, outre le secteur public fédéral (offices de la Confédération), également le secteur privé.

S'agissant des données de police judiciaire, elles sont régies par la LDPJu, qui confère à un juge du Tribunal cantonal la compétence de statuer sur leur consultation. Outre les dossiers de police judiciaire proprement dits, des données de nature judiciaire sont aussi contenues dans le Journal des événements police (JEP). Le JEP est toutefois une banque de données hybride, qui contient, de manière indissociable, à la fois des données de police judiciaire et des données qui ne le sont pas, celles-ci étant soumises au régime ordinaire de la LPrD. Par conséquent, l'Autorité cantonale de protection des données et de droit à l'information (APDDI ou, selon le texte actuel de la LPrD, "préposé(e)") a suggéré de profiter de la présente révision pour supprimer l'institution du juge cantonal chargé des dossiers de police judiciaire et de la remplacer par un système plus conventionnel, où le service responsable du traitement statue lui-même sur les demandes.

Cependant, un avis de droit, demandé par la préposée et émis par Sylvain Métile et Annelise Ackermann le 4 mars 2020, considère qu'une "possibilité de recourir à un droit d'accès indirect devrait être envisageable. Bien que la Directive 2016/680 oblige le responsable du traitement à accepter les demandes directes des personnes concernées, leurs droits peuvent être exercés par l'intermédiaire d'une autorité de contrôle [en l'occurrence le juge compétent au sens de la LDPju]. Cela implique que le responsable du traitement ne donne pas accès à la personne concernée, mais à une autorité tierce qui prend connaissance des données personnelles, qui vérifie si leur traitement est conforme, puis qui le confirme à la personne concernée. La personne concernée se voit accorder un accès à ses données que de manière différée ou limitée. Cette solution a été adoptée au niveau fédéral pour le système de traitement des données relatives aux infractions fédérales de la Police judiciaire fédérale (PJF) (…)".

Le système instauré par la LDPju correspond exactement à cette description. Il est ainsi conforme aux directives européennes et analogue à celui en vigueur au niveau fédéral. Il est donc renoncé à le modifier, d'autant plus qu'il semble fournir d'emblée des garanties supplémentaires en permettant le contrôle d'un organe neutre et indépendant sur le traitement de ces demandes. Quant au caractère mixte des données du JEP, un tri doit de toute façon se faire quelle que soit l'autorité intervenant, les données judiciaires étant quoi qu'il en soit soumises à un régime juridique différent que celles qui ne le sont pas. On relève par ailleurs que toute procédure en matière de protection des données implique de toute manière la compétence de plusieurs autorités. Par exemple, en matière de réclamation ou de recours, la Cour de droit administratif et public du Tribunal cantonal peut être saisie soit directement ou soit après le traitement d'un premier recours par la préposée, indifféremment.

A la demande du Tribunal cantonal, il a été renoncé à la création d'une autorité de recours intermédiaire, tout recours pouvant déjà être interjeté directement après des autorités citées.

Au surplus, le maintien de l'institution du juge cantonal chargé des dossiers de police judiciaire est préconisé à la fois par son titulaire actuel et par la Police cantonale, qui sont aujourd'hui les deux principales autorités concernées. Il présente par ailleurs, on l'a vu, des garanties particulières d'objectivité pour le justiciable. Quand bien même le Tribunal cantonal souhaiterait, dans l'idéal, décharger son juge de cette mission accessoire, une telle solution ne constituerait en réalité aucune économie globale pour l'Etat. Elle s'avérerait en outre conduire inévitablement à la création d'incertitudes juridiques et financières, qui doivent être évitées. La solution retenue correspond ainsi à un objectif pragmatique visant à conserver au public une procédure parfaitement viable sur le plan légal, y compris au regard des nouvelles normes européennes, et un système fonctionnant jusqu'ici de manière concrète à la satisfaction de tous.

## 2. Commentaire par articles de la LPrDS

### Titre : loi sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal

Le titre de la loi correspond à celui de la LPDS. Il reprend, en le résumant, celui de la directive (UE) 2016/680.

### Art. 1 : Champ d'application

La LPDS a circonscrit son champ d'application à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales dans le cadre de l'application de l'acquis de Schengen, et dans le cadre de l'application d'accords internationaux conclus avec l'Union européenne ou avec des Etats qui sont liés à la Suisse par l'un des accords d'association à Schengen (Etats Schengen) et qui renvoient à la directive (UE) 2016/680 pour ce qui est de la protection des données. Il en va de même sur le plan cantonal.

De surcroit, la LPDS prévoit, à son article 2, l'exclusion de son champ d'application aux droits des personnes concernées dans le cadre des procédures pendantes devant des tribunaux fédéraux ou dans le cadre de procédures pendantes régies par le code de procédure pénale ou par la loi du 20 mars 1981 sur l'entraide pénale internationale. Au niveau cantonal, les procédures pénales pendantes doivent aussi être expressément exclues du champ d'application de la présente loi, afin d'éviter un concours normatif, les dispositions du code de procédure pénale (CCP) ayant vocation à s'appliquer durant la procédure pénale (cf. art. 99 al. 1 CCP).

### Art. 2 Définitions

*Données génétiques et biométriques (art. 3 al. 1 litt. a ch. 3 et 4 LPDS)*

Les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN (art. 3 litt. l de la loi fédérale du 8 octobre 2014 sur l'analyse génétique humaine, LAGH).

Par données biométriques, on entend ici les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de la voix. Ces données doivent impérativement résulter d'un traitement technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel ne sera pas le cas, par exemple, de simples photographies.

*Profilage (art. 3 al. 1 litt. b LPDS)*

La notion de "profilage" s'ajoute dans la LPDS à celle de "profil de la personnalité". On la trouve aussi à l'art. 3 ch. 4 de la directive (UE) 2016/680. Les deux notions, bien que présentant de nombreuses similitudes, ne couvrent pas le même état de fait. Le profil de la personnalité est le résultat d'un traitement et traduit ainsi quelque chose de statique. A l'inverse, le profilage désigne une forme particulière de traitement, et constitue donc un processus dynamique. Ce dernier est par ailleurs toujours orienté vers une finalité particulière.

Le terme de profilage est adapté, sur le fond, à la terminologie européenne et ne recouvre que le traitement automatisé de données personnelles. Il est défini comme l'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée, afin notamment d'analyser ou de prédire sa situation économique, sa localisation, sa santé, son comportement, ses préférences ou ses déplacements. Autrement dit, le profilage se caractérise par le fait qu'on procède à une évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé. La loi cite quelques exemples de caractéristiques personnelles, telles la situation économique ou la santé. On peut en imaginer d'autres, comme le lieu de résidence. Les exemples mentionnés par la LPDS et relatifs au secteur privé n'ont cependant pas été repris ici, le champ d'application du droit cantonal se limitant au secteur public uniquement. On entend par évaluation automatisée toute évaluation fondée sur des techniques d'analyse informatisées. Le recours à des algorithmes est possible mais non constitutif du profilage. En revanche, l'évaluation automatisée des données est indispensable. La simple accumulation de données n'est pas assimilée au profilage.

L'évaluation automatisée vise en particulier à analyser ou à prédire certains comportements de la personne. Il est sans importance que celui qui procède au profilage le fasse pour lui ou pour le compte d'un tiers. Les données issues d'un profilage sont en principe des données personnelles au sens de l'art. 4 al. 1 ch. 1 LPrD qui, selon les circonstances, peuvent aussi constituer des données sensibles (art. 4 al. 1 ch. 2 LPrD).

*Décision individuelle automatisée (art. 3 al. 1 litt. d LPDS)*

Il y a décision individuelle automatisée lorsqu'une exploitation de données a lieu sans intervention humaine et qu'il en résulte une décision, ou un jugement, à l'égard de la personne concernée. Le fait que la décision soit au final communiquée par une personne physique ne change rien à son caractère automatisé, car cette personne n'a pas d'influence sur le processus de décision. La question déterminante est ainsi celle de savoir dans quelle mesure une personne physique peut faire un examen de la situation et se baser sur ses considérations pour rendre une décision finale. Cette décision doit cependant présenter un certain degré de complexité.

*Préposé*

Le Préposé au sens de la présente loi est l'autorité de protection des données et de droit à l'information, instituée par la LPrD sous le nom de "Préposé cantonal à la protection des données et à l'information" (ci-après le Préposé).

**Art. 3 Devoir d'informer la personne concernée en cas de décision individuelle automatisée**

Cette disposition correspond à l'art. 11 LPDS, qu'elle transpose sur le plan cantonal.

L'article 3 prévoit l'existence d'un devoir d'informer la personne concernée en cas de décision individuelle automatisée. Cette disposition remplit les exigences de l'art. 11 de la directive (UE) 2016/680. L'introduction de la notion de décision individuelle automatisée est nécessaire car ces décisions sont de plus en plus fréquentes en raison du développement technologique.

*Al. 1 Information*

Selon l'alinéa 1 Le responsable du traitement informe la personne concernée de toute décision individuelle automatisée (art. 2 al. 4) prise à son égard; il qualifie cette décision comme telle.
Cela implique dans tous les cas qu'il n'y ait eu aucune décision prise par une personne physique sur la base de sa propre évaluation de la situation.
Il n'est pas nécessaire que la personne concernée soit informée de chaque décision individuelle automatisée, mais seulement lorsque la décision a pour elle des effets juridiques ou l'affecte de manière significative. Dans le domaine du droit public, il y a effets juridiques lorsqu'une décision découle d'une décision individuelle automatisée, comme par exemple une taxation fiscale automatique.
On peut supposer que la personne concernée est affectée de manière significative lorsqu'elle est durablement entravée sur le plan économique ou personnel. Une simple nuisance ne suffit pas. Tout dépend des circonstances concrètes du cas d'espèce. Il faut en particulier tenir compte de l'importance du bien en question pour la personne concernée, de la durée des effets de la décision et de l'existence ou non d'une solution de remplacement.
Le responsable du traitement doit aussi informer la personne concernée en cas de profilage, si celui-ci entraîne une décision qui aura pour elle des effets juridiques ou qui l'affectera de manière significative.

*Al. 2 Exposition du point de vue*

Selon l'alinéa 2, si la personne concernée le demande, Le responsable du traitement lui donne la possibilité de faire valoir son point de vue. La personne concernée peut exiger que la procédure appliquée lui soit communiquée et que la décision soit revue par une personne physique.
Le responsable du traitement doit donner à la personne concernée, si elle le demande, la possibilité de faire valoir son point de vue sur le résultat de la décision, et même de demander comment la décision a été prise. Le but est entre autres d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes. Cette règle est également dans l'intérêt du responsable du traitement, pour lequel une décision individuelle automatisée erronée peut avoir des conséquences négatives.

La loi ne précise pas à quel moment la personne concernée doit être informée ni quand elle a la possibilité d'exposer son point de vue. Cela peut donc se faire avant ou après la décision. Il est ainsi notamment possible de lui notifier une décision individuelle automatisée – qui sera désignée comme telle – et de l'entendre dans le cadre de l'exercice du droit d'être entendu, ou lors d'une procédure de recours. Cela ne doit toutefois pas engendrer de frais supplémentaires trop élevés (par ex. des frais de procédure), qui dissuaderaient la personne concernée d'exercer ses droits.

*Al. 3 Exception*

L'alinéa 3 dispose que le devoir d'informer et d'entendre la personne concernée ne s'applique pas lorsque la personne concernée dispose d'une voie de droit contre la décision.
La personne concernée dispose en principe d'un droit de recours (par défaut : articles 92 et suivants de la loi du 28 octobre 2008 sur la procédure administrative, LPA), voire d'une procédure de réclamation (art. 66 ss LPA). Elle peut donc faire valoir son point de vue et faire examiner la décision par une personne physique. En d'autres termes, les droits garantis par l'art. 3 al. 1 et 2 du présent projet le sont déjà par ces voies de droit.

**Art. 4 Protection des données dès la conception et par défaut**

Cette disposition correspond à l'art. 5 LPDS, qu'elle transpose sur le plan cantonal.

L'article 4 du présent projet instaure l'obligation de protéger les données dès la conception et par défaut. Cette disposition met en œuvre les exigences de l'art 20, § 1, de la directive (UE) 2016/680.

*Al. 1 Protection des données dès la conception*

L'alinéa 1 impose au responsable du traitement de concevoir dès l'origine le traitement de données de telle manière qu'il respecte les prescriptions relatives à la protection des données. La nouvelle obligation repose sur le principe de la technologie au service de la protection des données personnelles (*privacy by design*). Le recours à des solutions techniques pour garantir la protection des données s'appuie sur l'idée que la technologie et le droit se complètent. Ainsi, des solutions techniques qui rendent impossible une violation de la protection des données ou qui en réduisent la probabilité rendent les règles juridiques et les codes de conduite moins nécessaires. Par ailleurs, ces technologies sont indispensables pour mettre en œuvre les réglementations de protection des données. Le traitement de données personnelles est omniprésent à bien des égards et va encore s'amplifier (*ubiquitous computing*). Il en résulte des quantités de données personnelles gigantesques, qu'il faut traiter dans le respect des dispositions légales. Or cela est impossible sans des solutions techniques adaptées. La protection technique des données personnelles ne s'appuie pas sur une technologie précise; elle passe plutôt par la mise en place de règles techniques et organisationnelles conformes aux principes définis par cet article. En d'autres termes, les exigences légales auxquelles doit satisfaire un traitement conforme à la protection des données sont déjà intégrées dans le système, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité. Il s'agit par exemple de la fixation d'échéances régulières pour l'effacement ou l'anonymisation systématique des données personnelles. Un principe significatif pour la protection des données au plan technique est celui de la minimisation des données, qui ressort aussi de cet article. Selon celui-ci, il faut fixer avant même le début d'un traitement ses modalités, de manière à ce que le moins de données possible soient traitées, et de façon à ce qu'elles soient conservées le moins longtemps possible.

*Al. 2 Caractère approprié des mesures*

L'alinéa 2 précise les exigences auxquelles doivent satisfaire les mesures visées à l'alinéa 1. Ces mesures doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue et du degré de probabilité et de gravité du risque que le traitement des données en question présente pour la personnalité et les droits fondamentaux des personnes concernées.

La norme matérialise l'approche fondée sur les risques. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées.

*Al. 3 Protection des données par défaut*

Selon l'alinéa 3, le responsable du traitement est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie (*privacy by default*). Les mesures en question résident dans des réglages prédéfinis (par ex. l'installation d'un logiciel) qui s'appliquent de manière standardisée. Ces paramètres standards peuvent être effectués en usine ou ultérieurement (par ex. définir, pour un ordinateur, une imprimante par défaut). Dans le contexte de la protection des données, cela signifie que le processus de traitement doit être préprogrammé de manière à garantir autant que possible la protection des données.

La protection des données par défaut joue un rôle mineur dans le secteur public, car les traitements y reposent moins sur le consentement de la personne concernée que sur des obligations légales.

Le responsable du traitement peut montrer, par une certification ou une analyse d'impact relative à la protection des données notamment, qu'il respecte les obligations définies dans cette disposition.

**Art. 5 Principe de légalité**

En vertu du principe de légalité inscrit à l'art. 5, al. 1, Cst., toute action de l'Etat (y compris le traitement ou la communication de données) nécessite une base légale (voir aussi les art. 13, al. 2, 27 et 36 Cst.).

Le principe de légalité impose donc qu'une base légale formelle légitime tout mode de traitement susceptible de porter gravement atteinte aux droits fondamentaux, s'agissant de données personnelles sensibles.

Il ne peut y avoir exception à cette exigence d'une base légale que si, alternativement, il existe un besoin de protection de la vie de la personne concernée, si cette personne a rendu publiques ses données ou si elle ne s'est pas opposée à leur traitement.

Selon le rapport explicatif de la LPDS, le profilage est considéré comme un "traitement susceptible de porter gravement atteinte aux droits fondamentaux des personnes concernées (art. 36 Cst.)" (cf. p. 8 du rapport et commentaire de l'art. 6, al. 2, let. c, LPDS). Au niveau fédéral, le profilage doit ainsi reposer sur une base légale au sens formel, comme cela ressort de l'art. 6, al. 2, let. c, LPDS. Tel doit également le cas au niveau cantonal vaudois.

**Art. 6 Registre des activités de traitement**

Cet article reprend le contenu de l'art. 12 LPDS en l'adaptant au contexte cantonal.

Pour mémoire, les responsables du traitement tiennent un registre des activités de traitement.
Le registre du responsable de traitement contient au moins les indications suivantes : le nom du responsable du traitement; la finalité du traitement; une description des catégories des personnes concernées et des catégories des données personnelles traitées; les catégories des destinataires; la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour déterminer la durée de conservation; dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données; l'Etat tiers ou l'organisme international auquel des données personnelles sont communiquées ainsi que les garanties de protection des données personnelles prévues.

**Art. 7 Analyse d'impact**

Cette disposition correspond à l'art. 13 LPDS, qu'elle transpose sur le plan cantonal.

L'article 7 du présent projet instaure une obligation de procéder à une analyse d'impact relative à la protection des données personnelles. Cette disposition concrétise les exigences posées aux articles 27 et suivants de la directive (UE) 2016/680.

La définition et le rôle de l'analyse d'impact résultent de l'art. 7 al. 3 du présent projet. Il s'agit d'un instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour la personne concernée. Le cas échéant, cette analyse doit servir à définir des mesures pour faire face à ces risques. L'avantage pour le responsable du traitement est qu'elle permet d'anticiper d'éventuels problèmes juridiques liés à la protection des données et d'éviter les coûts qui pourraient en résulter.

Al. 1 et 2 Motifs justifiant la réalisation d'une analyse d'impact

L'alinéa 1 prévoit que le responsable du traitement procède à une analyse d'impact lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux de la personne concernée. Le responsable du traitement est donc tenu de faire un pronostic des conséquences que le traitement en question peut avoir pour la personne concernée. Sont déterminants, notamment, la nature et l'ampleur de l'impact du traitement sur les droits fondamentaux de la personne concernée.

Le droit à l'autodétermination en matière informationnelle et le droit à la sphère privée notamment permettent de cerner le risque en question. Ces droits protègent l'autodétermination de la personne concernée, de même que sa dignité et son identité. Dans le domaine de la protection des données, l'autonomie se traduit principalement par la possibilité de disposer soi-même de ses données personnelles, sans devoir craindre qu'elles ne se trouvent en quantité indéterminée aux mains d'une multitude de tiers pouvant en faire ce qu'ils veulent. Les données sont étroitement liées à l'identité d'une personne. Quiconque dispose de données sur une personne et les combine peut en faire ressortir des détails intimes, qu'elle n'aurait sans doute accepté de révéler qu'à une personne très proche. Ce problème ne concerne pas seulement la liberté de chacun de disposer de ses données personnelles : les données dont on dispose sur une autre personne peuvent influencer de bien des manières ses relations avec son entourage, le cas échéant sans qu'elle en connaisse la raison. Le fait de savoir qu'elle est observée peut même amener la personne à modifier son comportement. Enfin, le détenteur des informations pourrait être tenté de les utiliser à des fins susceptibles de porter gravement atteinte à la dignité de la personne concernée.

Pour évaluer le risque, le responsable du traitement doit faire un lien entre, d'une part, le traitement envisagé et, d'autre part, le droit à l'autodétermination informationnelle de la personne concernée ainsi que son droit à sa sphère privée. Il s'agit donc de prendre en considération le traitement des données au regard de l'autodétermination, de l'identité et de la dignité de la personne concernée. On peut admettre l'existence d'un risque élevé lorsqu'il apparaît que les propriétés du traitement envisagé ont – ou pourraient avoir – pour effet de restreindre dans une large mesure la liberté de la personne de disposer de ses données. Ce risque élevé peut résulter, par exemple, de la nature ou du contenu des données à traiter (par ex. données sensibles), de la nature ou de la finalité du traitement envisagé (par ex. profilage), de la quantité de données à traiter, de leur transmission vers un Etat tiers (par ex. si le droit de l'Etat en question ne garantit pas un niveau de protection adéquat) ou de ce que les données seraient accessibles à un grand nombre, voire à un nombre illimité, de personnes.

L'alinéa 2 de cet article précise que l'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Plus le traitement est étendu, plus les données sont sensibles et plus la finalité du traitement est vaste, plus il y a lieu de conclure à un risque élevé. L'alinéa 2 mentionne deux exemples dans lesquels un tel risque existe : selon la *lettre a*, c'est le cas lorsque le traitement concerne un grand volume de données sensibles, comme cela peut se produire dans le cadre de projets de recherche, par exemple. La *lettre b* dispose qu'un risque élevé existe en cas de profilage. Tel peut être également le cas lorsque des décisions sont prises exclusivement sur la base d'un traitement de données personnelles automatisé, y compris en cas de profilage, et que ces décisions ont des effets juridiques sur la personne concernée ou l'affectent de manière notable. Il ne faut pas perdre de vue en effet que ce type de décisions peuvent, selon le cas, avoir des répercussions non négligeables pour la personne concernée. Une analyse d'impact est également nécessaire dans de telles situations.

La *2e phrase* de l'alinéa 1 autorise le responsable du traitement à effectuer une analyse d'impact commune s'il envisage d'effectuer plusieurs opérations de traitement semblables. Sont visés en particulier les traitements poursuivant un objectif supérieur commun. En pareil cas, il n'est pas nécessaire d'examiner individuellement chacune des étapes prévues sur une plateforme de traitement. L'analyse d'impact peut porter sur la plateforme dans son ensemble.

*Al. 3 Contenu de l'analyse d'impact relative à la protection des données personnelles*

Selon l'alinéa 3 de cet article, l'analyse d'impact relative à la protection des données doit tout d'abord exposer le traitement envisagé. Il faut ainsi présenter les différents processus (par exemple la technologie employée), la finalité du traitement ou la durée de conservation des données personnelles. Par ailleurs, l'analyse d'impact doit montrer quels risques le traitement implique pour la personnalité ou les droits fondamentaux de la personne concernée. Il s'agit ici d'un approfondissement de l'évaluation des risques qui doit déjà être faite en amont, lors de l'examen de la nécessité de procéder à une analyse d'impact. Il convient ainsi de présenter la nature du risque élevé qu'engendre le traitement envisagé et les moyens de l'évaluer. Enfin, l'analyse d'impact doit expliquer les mesures prévues pour faire face à ce risque. Il s'agira souvent de mettre en œuvre les principes des articles 5 à 12 LPrD, ainsi que les principes de protection dès la conception et par défaut (*privacy by design/by default*; art. 4 du présent projet). A cette occasion, il est possible de mettre en balance les intérêts de la personne concernée et ceux du responsable du traitement. Cette confrontation des intérêts doit être dûment motivée et intégrée dans l'analyse d'impact.

**Art. 8 Consultation du Préposé**

Cette disposition correspond à l'art. 14 LPDS, qu'elle transpose sur le plan cantonal.

*Al. 1 Obligation de consulter le Préposé*

Aux termes de l'alinéa 1, le responsable du traitement doit obtenir une prise de position du Préposé préalablement au traitement s'il ressort de l'analyse d'impact que le traitement envisagé présenterait un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée si aucune mesure n'était prise. Cette consultation préalable correspond à la réglementation européenne (art. 28 de la directive [UE] 2016/680). Elle est reprise dans le présent projet pour permettre au Préposé d'exercer une fonction de conseil et de prévention, sans compter qu'elle offre une plus grande efficacité aux responsables du traitement en ce sens que les difficultés qui pourraient surgir en lien avec le traitement sont déjà éliminées à un stade précoce.

*Al. 2 et 3 Objections du Préposé*

Le Préposé a deux mois suivant la réception de la communication pour communiquer au responsable du traitement ses objections concernant le traitement et les mesures envisagés. Dans des cas particulièrement compliqués, ce délai peut être prolongé d'un mois. Si le responsable ne reçoit pas de nouvelles du Préposé dans le délai de deux mois, il peut partir du principe que le Préposé n'a pas d'objections contre les mesures envisagées.

Lorsqu'il est informé du résultat d'une analyse d'impact, le Préposé vérifie si les mesures proposées sont suffisantes pour protéger la personnalité et les droits fondamentaux de la personne concernée. S'il arrive à la conclusion que le traitement contreviendrait, dans la forme envisagée, aux dispositions de la protection des données, il propose des mesures appropriées au responsable du traitement.

Le Préposé n'en reste pas moins libre d'ouvrir une enquête ultérieurement si les conditions de l'art. 12 du présent projet sont remplies, en particulier s'il apparaît que les risques n'ont pas été correctement évalués dans le cadre de l'analyse d'impact et que, par conséquent, les mesures définies ratent leur cible ou sont insuffisantes.

**Art. 9 Annonce des violations de la sécurité des données**

Cette disposition correspond à l'art. 15 LPDS, qu'elle transpose sur le plan cantonal.

L'article 9 du présent projet instaure l'obligation d'annoncer toute violation de la sécurité des données personnelles. Cette disposition concrétise les exigences fixées aux articles 30 et suivants de la directive (UE) 2016/680.

*Al. 1 Notion et fondements*

L'alinéa 1 dispose que le responsable du traitement annonce au Préposé dans les meilleurs délais toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour les droits fondamentaux de la personne concernée.

Par "violation de la sécurité des données", on entend toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, qui entraîne la perte de données personnelles, leur modification, leur effacement ou leur destruction, ou encore leur divulgation ou un accès non autorisés. La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences ou qui fait preuve de négligence. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut aussi engendrer une violation de la personnalité, par exemple en entraînant la divulgation d'informations que la personne souhaitait garder secrètes. Cette définition est formulée in extenso à l'article 2 de la loi.

La personne concernée ne peut réagir à ces menaces que si elle sait que la sécurité des données a été violée. C'est pourquoi le responsable du traitement doit annoncer tout traitement non autorisé au Préposé en premier lieu et, si les conditions de l'alinéa 4 sont remplies, à la personne concernée également. L'annonce doit avoir lieu dans les meilleurs délais à partir du moment où le traitement non autorisé est connu. Le responsable du traitement doit en principe agir rapidement, mais la disposition lui laisse une certaine marge d'appréciation, qui dépend en pratique de l'ampleur du risque pour la personne concernée. Plus ce risque est élevé et le nombre de personnes concernées important, plus son intervention doit être rapide. L'annonce au Préposé n'est toutefois nécessaire que s'il est vraisemblable que la violation de la sécurité des données entraînera un risque élevé pour les droits fondamentaux de la personne concernée. Il s'agit d'éviter l'annonce de violations insignifiantes. Le responsable du traitement doit évaluer dans tous les cas les conséquences possibles de la violation pour la personne concernée.

*Al. 2 Contenu de l'annonce*

L'alinéa 2 précise les indications que l'annonce au Préposé doit contenir au minimum. Le responsable du traitement doit tout d'abord indiquer la nature de la violation, pour autant que cela lui soit possible. On distingue quatre types de violations : l'effacement ou la destruction de données, leur perte, leur modification ou leur communication à des tiers non autorisés.

L'annonce doit aussi expliquer, dans la mesure du possible, les conséquences de la violation de la sécurité des données. Ce sont avant tout les conséquences pour la personne concernée et non les conséquences pour le responsable du traitement qui sont visées ici.

Enfin, il y a lieu de préciser également les mesures prises ou envisagées pour remédier à la violation de la sécurité des données ou pour atténuer ses conséquences. L'annonce doit permettre dans tous les cas au Préposé d'intervenir le plus rapidement et le plus efficacement possible.

*Al. 3 Annonce par le sous-traitant*

La violation de la sécurité des données peut aussi se produire chez un éventuel sous-traitant, qui veille, le cas échéant, à informer le responsable du traitement dans les meilleurs délais de tout traitement non autorisé. Il revient ensuite au responsable du traitement de procéder à une évaluation des risques et de décider si une notification au Préposé et à la personne concernée s'impose.

*Al. 4 Information de la personne concernée*

Selon l'alinéa 4, la personne concernée ne doit être informée que si les circonstances le requièrent ou si le Préposé l'exige. Il existe une marge d'appréciation assez large pour déterminer si la première condition est réalisée. Il faut se demander notamment si l'information peut réduire les risques pour la personnalité ou les droits fondamentaux de la personne concernée, en lui permettant notamment de prendre les dispositions nécessaires pour se protéger.

*Al. 5 Restrictions du devoir d'informer la personne concernée*

L'alinéa 5 dispose que le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer dans un certain nombre de cas que cette disposition énumère.

La *lettre d* admet notamment une restriction de l'information s'il n'est pas possible de respecter le devoir d'informer ou si l'information nécessiterait des efforts disproportionnés.

Le devoir d'informer est réputé impossible à respecter lorsque le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données, par exemple parce que les fichiers journaux qui permettraient une identification ne sont plus disponibles, ou parce que ces personnes ne sont pas domiciliées dans la circonscription du responsable du traitement, voire domiciliées dans un autre canton ou à l'étranger, sans que ce domicile soit par ailleurs déjà connu. On estime de même que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées. C'est notamment dans ces cas de figure que peut s'appliquer la *lettre e* : cette disposition autorise le responsable du traitement à opter pour une communication publique si l'information des personnes concernées est garantie de manière équivalente. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée.

**Art. 10 Conseiller à la protection des données**

Cette disposition correspond à l'art. 16 LPDS, qu'elle transpose sur le plan cantonal.

Dans l'espace Schengen, Les responsables du traitement sont obligés, conformément à l'article 32 de la directive (UE) 2016/680, de nommer un conseiller (ou "délégué") à la protection des données.

Le conseiller à la protection des données veille au respect des prescriptions de protection des données au sein d'une entité et prodigue au responsable du traitement des conseils en matière de protection des données. Le responsable du traitement est cependant le seul responsable du traitement en bonne et due forme des données personnelles.

*Al. 1 et 2 Désignation*

Le responsable du traitement peut nommer conseiller à la protection des données un collaborateur ou un tiers.

Selon la *lettre a*, le conseiller à la protection des données doit avoir les connaissances professionnelles nécessaires pour exercer cette tâche, s'agissant notamment de la législation en matière de protection des données et des normes techniques relatives à la sécurité des données.

La *lettre b* interdit au conseiller à la protection des données d'exercer des tâches incompatibles avec sa mission. Rien n'interdit toutefois, en principe, d'imaginer qu'un conseiller à la protection des données puisse être en même temps délégué à la sécurité de l'information.

Le conseiller à la protection des données est un interlocuteur important, aussi bien pour la personne concernée que pour le Préposé, en ce qui concerne le traitement de données par l'organe en question.

**Art. 11 Prétentions et procédure**

L'art. 19 LPDS introduit une nouvelle réglementation issue de la directive (UE) 2016/680, afin que le responsable de traitement procède à une limitation de traitement des données litigieuses. Quand bien même, si au regard des dispositions des art. 27 ss LPrD, il semble possible en droit positif cantonal de limiter le traitement des données litigieuses, il apparaît plus opportun et plus clair d'intégrer cette mesure dans le présent projet de loi.

**Art. 12 Enquête du Préposé**

Cette disposition correspond à l'art. 22 LPDS, qu'elle transpose sur le plan cantonal.

*Al. 1 Ouverture de l'enquête*

En vertu de l'art. 12 al. 1, le Préposé est tenu d'ouvrir une enquête d'office ou sur dénonciation dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données. Le dénonciateur peut être un tiers ou la personne concernée. Il n'a toutefois pas qualité de partie à la procédure. En revanche, si c'est la personne concernée qui est l'auteur de la dénonciation, le Préposé est tenu de l'informer de la suite donnée à sa dénonciation (al. 4). Au surplus, pour faire valoir ses droits, la personne concernée doit agir selon les voies de droit applicables, à savoir par voie de recours contre la décision rendue par le responsable du traitement, comme c'est du reste déjà le cas aujourd'hui.

*Al. 2 Renonciation à l'ouverture d'une enquête*

Le Préposé peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance. Tel serait le cas par exemple si l'on a envoyé un e-mail en omettant de cacher l'identité des destinataires. L'alinéa 2 peut également s'appliquer si le Préposé considère que la fourniture de conseils au responsable du traitement concerné peut constituer une mesure suffisante pour remédier à une situation en soi peu problématique.

*Al. 3 Devoirs de collaboration*

L'alinéa 3 règle le devoir de collaboration du responsable du traitement. En vertu de cette disposition, la partie à la procédure d'enquête doit fournir au Préposé tous les renseignements et documents qui lui sont nécessaires pour son enquête.

**Art. 13 Pouvoirs du Préposé**

Cette disposition correspond à l'art. 23 LPDS, qu'elle transpose sur le plan cantonal.

L'art. 47, § 1, de la directive (UE) 2016/680 prescrit que les Etats Schengen sont tenus de prévoir que l'autorité de contrôle dispose de pouvoirs d'enquête, notamment celui d'obtenir du responsable du traitement l'accès à toutes les données traitées et à toutes les informations nécessaires pour l'exercice de ses tâches.

*Al. 1 Mesures d'investigation*

Les mesures énumérées à l'alinéa 1 ne peuvent être ordonnées que si une procédure d'enquête a été ouverte et pour autant que le responsable du traitement ne respecte pas son obligation de collaborer. En d'autres termes, ce n'est que si ses tentatives d'obtenir la collaboration du responsable du traitement sont restées vaines que le Préposé pourra ordonner les mesures prévues aux litt. a à d.

Le catalogue des mesures prévues à l'alinéa 1 est semblable à celui de l'art. 29 LPA. Il s'agit d'une liste non exhaustive. Parmi les attributions, le Préposé peut ordonner l'accès à tous les renseignements, documents, registres d'activités et données personnelles nécessaires pour l'enquête (*litt. a*) ou encore l'accès aux locaux et aux installations (*litt. b*). Comme toute autorité cantonale, le Préposé doit respecter les dispositions légales applicables, notamment celles de protection des données et celles garantissant la confidentialité des secrets d'affaires et de fabrication. Il est également soumis au secret de fonction au sens de l'article 18 de la loi du 24 septembre 2002 sur l'information (LInfo). La confidentialité des données personnelles auxquelles il a accès dans l'exercice de ses tâches de surveillance est ainsi garantie, notamment lorsqu'il informe l'auteur d'une dénonciation de la suite donnée à celle-ci (art. 12 al. 4) ou lorsqu'il publie son rapport d'activité en vertu de l'art. 40 LPrD.

*Al. 2 Mesures provisionnelles*

Cette disposition confère au Préposé la compétence d'ordonner des mesures provisionnelles pour la durée de l'enquête. La procédure de recours contre les mesures provisionnelles est régie par la LPA (cf. art. 74 al. 3 LPA).

**Art. 14 Mesures administratives**

Cette disposition correspond à l'art. 24 LPDS, qu'elle transpose sur le plan cantonal.

L'article 14 du présent projet met en œuvre l'art. 47, § 2, de la directive (UE) 2016/680 et donne suite aux recommandations des évaluateurs Schengen de conférer des compétences décisionnelles au Préposé.

Cette disposition laisse une grande marge de manœuvre au Préposé. En effet, elle ne l'oblige pas à prendre des mesures administratives, mais lui donne la faculté de le faire.

Les mesures prévues vont du simple avertissement (al. 3) jusqu'à l'ordre de détruire des données personnelles (al. 1) ou à l'interdiction de communiquer des données personnelles à l'étranger (al. 2). Le principe de base de cette réglementation est le respect du principe de proportionnalité.

Ainsi, au lieu d'ordonner la cessation du traitement, le Préposé peut ordonner sa modification et limiter la mesure à la partie du traitement problématique. Il peut également se limiter à prononcer un avertissement si la partie à l'enquête a pris les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données (al. 3).

Le Préposé notifie sa décision conformément à la procédure administrative (renvoi général à la loi du 18 octobre 2008 sur la procédure administrative – LPA - contenu dans l'art. 16 al. 2 du présent projet de loi). La mesure prononcée doit être motivée de manière précise. Le responsable du traitement concerné doit en effet être en mesure de déterminer les traitements tombant sous le coup de la décision du Préposé. Les parties à la procédure d'enquête ont qualité pour recourir, conformément aux dispositions générales sur la procédure administrative qui s'appliquent pour le surplus (al. 4 et 5).

**Art. 15 Assistance administrative internationale**

Cette disposition règle l'assistance administrative entre le Préposé et les autorités étrangères des Etats Schengen chargées de la protection des données. Cette disposition transpose dans le droit cantonal l'art. 26 LDPS, qui correspond à l'article 50 de la directive (UE) 2016/680.

*Al. 1 Conditions*

Cette disposition pose le principe selon lequel le Préposé peut échanger des données personnelles avec une autorité étrangère chargée de la protection des données pour l'accomplissement de leurs tâches légales respectives, pour autant que certaines conditions, énumérées aux litt. a à e, soient remplies.
Selon la première condition (litt. a), le principe de réciprocité en matière d'assistance administrative dans le domaine de la protection des données doit être garanti entre la Suisse et l'Etat Schengen. Deuxièmement, conformément au principe de spécialité, les informations et les données personnelles échangées ne doivent être utilisées que dans le cadre de la procédure liée à la protection des données à la base de la demande d'assistance (litt. b). Si les données transmises doivent être utilisées ultérieurement dans le cadre d'une procédure pénale, les dispositions sur l'entraide judiciaire internationale en matière pénale s'appliquent. Les troisième et quatrième conditions garantissent le respect des secrets professionnels, d'affaires et de fabrication (litt. c) et interdisent que les informations et les données échangées soient communiquées à des tiers sans l'accord préalable de l'autorité qui les a transmises (litt. d). Enfin, l'autorité destinataire doit respecter les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations (litt. e).
Le Préposé doit refuser la demande d'assistance administrative d'une autorité d'un autre Etat Schengen par exemple si les conditions citées ne sont pas respectées.

*Al. 2 Communication de données personnelles*

L'alinéa 2 définit aux litt. a à g les informations que le Préposé peut communiquer à l'autorité étrangère pour motiver sa demande d'assistance administrative ou pour donner suite à une demande étrangère. L'identité des personnes concernées peut être communiquée si cela est indispensable à l'accomplissement des tâches légales du Préposé ou de l'autorité étrangère (litt. c).

*Al. 3 Consultation*

Lorsque, dans le cadre d'une procédure d'assistance administrative, le Préposé envisage de transmettre à une autorité étrangère chargée de la protection des données des informations susceptibles de contenir des secrets professionnels ou des secrets d'affaires ou de fabrication, il est tenu d'informer les personnes concernées en les invitant à prendre position. Le Préposé est néanmoins délié de son obligation si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés.

**Art. 16 Dispositions supplétives**

L'élaboration du présent projet de loi a été coordonnée avec une révision globale du droit cantonal en matière de protection des données. Il peut ainsi être fait renvoi, pour compléter le dispositif prévu ici aux autres lois existantes dont le champ d'application recoupe la loi sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal.

**Art. 17 exécution et entrée en vigueur**

L'art. 17 reprend la formule usuelle d'exécution.

## 3. Commentaire de la modification de la LPrD

Selon l'APDDI, dans sa formulation actuelle, l'article 3 alinéa 3 lettre c LPrD dernière partie "et de l'article 2, alinéa 1 de la loi sur les dossiers de police judiciaire" empêche, en théorie, d'appliquer la LPrD, même le cas échéant à titre supplétif, aux dossiers de police judiciaire. Cette disposition est donc trop restrictive, particulièrement en regard des accords de Schengen, la LPrDS proposée renvoyant d'ailleurs parfois expressément à la loi plus générale qu'est la LPrD. Au surplus, la suppression d'une réserve expresse de la LDPJu dans la LPrD ne remet pas en cause l'existence de la LDPJu : cette réserve était seulement inadéquate du point de vue de la technique législative. En effet, il n'est pas nécessaire de réserver expressément dans la LPrD toutes les lois spéciales, au risque d'en omettre. Au contraire, ce sont ces lois spéciales qui doivent renvoyer à la LPrD, qui sera applicable à titre de droit supplétif, pour combler leurs éventuelles lacunes, ainsi qu'il est procédé dans le présent projet au sein de la LDPJu elle-même.

## 4. Commentaire des modifications de la LDPJu, par articles

**Art. 1 Définition**

*Alinéa 1*

D'une part, cette disposition doit être complétée pour inclure aussi le droit cantonal ou communal.

D'autre part, l'exception du registre des contraventions de circulation doit être supprimée. Il s'agit en effet d'éviter un traitement différencié des données au sein d'un même dossier, avec des risques de décisions contradictoires.

*Alinéa 2*

La terminologie employée est actualisée et prend un sens plus large, indispensable aujourd'hui, la notion d' "imagerie" remplaçant celle de "photographie".

**Art. 2 al. 2 Contenu des dossiers**

Il paraît opportun de préciser que les données concernant l'orientation sexuelle d'une personne font aussi partie de cette catégorie, qui correspond aux données personnelles sensibles visées par les autres lois de protection des données.

**Art. 8 al. 1 Modalités**

La notion de "suppression" est ajoutée, en référence notamment à la loi du 14 juin 2011 sur l'archivage. En effet, celle-ci concrétise le principe de la proportionnalité en protection des données, en imposant aux responsables du traitement d'observer un calendrier de conservation.

**Art. 8a**

*Titre : droit aux renseignements ou à la constatation d'un traitement illicite de donnés*

*Alinéa 1a (nouveau)*

Doit être prévue la possibilité de constater le traitement illicite de donnés. La formulation est reprise de l'article 29 LPrD.

**Art. 8b Autorités compétentes**

*Alinéa 1*

Voir commentaire ad art. 8a al. 1a.

**Art. 8c Procédure**

La procédure garantit un accès effectif aux pièces et données personnelles figurant au dossier de police judiciaire par la personne concernée; de même que l'accès aux renseignements prévus par l'article 14 de la Directive UE 2016/680. En conséquence, le Juge unique du TC devra garantir un accès effectif aux données personnelles de la personne concernée et aux renseignements tels que visés par l'article 14 de la Directive UE 2016/680, sous réserve de l'existence d'un intérêt privé ou public prépondérant. Le secret prévu par l'art. 5 de la présente loi n'est en aucun cas opposable à la personne concernée lorsqu'elle exerce son droit d'accès.

*Alinéa 1*

Le nouvel art. 8b al. 1 mentionnera désormais la demande de constatation du caractère illicite d'un traitement, raison pour laquelle le projet propose de compléter en ce sens le présent alinéa.

*Alinéa 3*

La procédure est ici reprise de l'art. 12 al 4 de la directive UE.
*Alinéa 5*

La mention de la décision positive est supprimée, dans la mesure où celle-ci peut revêtir plusieurs formes et où une mention est ici inutile.
La dernière phrase est également supprimée, sa formulation ne reflétant plus la réalité et pouvant donc induire en erreur. D'une part, une décision rendue sur le plan cantonal n'est jamais définitive, puisque susceptible de recours au Tribunal fédéral. D'autre part, des voies de recours internes au canton doivent être prévues avant l'accès au Tribunal fédéral (art. 86 de la loi du 17 juin 2005 sur le Tribunal fédéral).

*Alinéa 6*

Cette précision est nécessaire car la voie de recours auprès du préposé de l'art. 31 LPrD, applicable à titre supplétif, n'est pas souhaitée.

**Art. 8d**

*Titre : droit de rectification ou de suppression*

Voir commentaire ad art. 8 al. 1 ci-dessus. La personne doit pouvoir demander non seulement la rectification, mais le cas échéant aussi la suppression de certaines données.

*Alinéa 1*

Voir commentaire ad art. 8 al. 1 ci-dessus et ad titre de l'art 8d. Est ajoutée la possibilité de demander aussi la suppression de certaines données.

*Alinéa 6*

A l'instar de ce qui est le cas pour l'art. 8c al. 5 (voir ci-dessus) la dernière phrase, mentionnant le caractère définitif de la décision du juge, doit être supprimée. En effet des voies de recours fédérales et cantonales existent bel et bien (notamment et par défaut, en droit cantonal, le recours de droit administratif des art. 92 ss LPA).

**Art. 8g (nouveau) Droit supplétif**

La loi sur la protection des données et la loi sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal s'appliquent à titre supplétif.

## 5. CONSEQUENCES

### 5.1. Constitutionnelles, légales et réglementaires (y.c. eurocompatibilité)

Actes législatifs assurant l'eurocompatibilité du droit vaudois avec les accords de Schengen.

### 5.2 Financières (budget ordinaire, charges d'intérêt, autres)

Salaire et équipement d'un conseiller à la protection des données (rattachement, statut et taux d'activité à définir).

### 5.3. Conséquences en termes de risques et d'incertitudes sur les plans financier et économique

Néant.

### 5.4. Personnel

Désignation d'un conseiller à la protection des données.

### 5.5. Communes

Néant.

### 5.6. Environnement, développement durable et consommation d'énergie

Néant.

### 5.7. Programme de législature et PDCn (conformité, mise en œuvre, autres incidences)

Néant.

### 5.8 Loi sur les subventions (application, conformité) et conséquences fiscales TVA

Néant.

### 5.9. Découpage territorial (conformité à DecTer)

Néant.

### 5.10. Incidences informatiques

Néant.

### 5.11. RPT (conformité, mise en œuvre, autres incidences)

Néant.

### 5.12. Simplifications administratives

Néant.

### 5.13. Protection des données

Fournit un cadre légal à la protection des données dans le domaine de compétence vaudois par rapport à l'application des accords de Schengen.

### 5.14. Autres

Néant.

## 6. CONCLUSION

Vu ce qui précède, le Conseil d'Etat a l'honneur de proposer au Grand Conseil d'adopter le projet de loi :

- sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal
- modifiant la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD)
- modifiant la loi du 1er décembre 1980 sur les dossiers de police judiciaire (LDPJu)

# PROJET DE LOI
# sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal du 6 juillet 2022

LE GRAND CONSEIL DU CANTON DE VAUD

en exécution de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

vu l'avant-projet de loi présenté par le Conseil d'Etat

*décrète*

## Titre I Dispositions générales

### Art. 1 Champ d'application

[1] La présente loi concerne la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales dans le cadre de l'application de l'acquis de Schengen et dans le cadre de l'application d'accords internationaux conclus avec l'Union européenne ou avec des Etats qui sont liés à la Suisse par l'un des accords d'association à Schengen (Etats Schengen).

[2] La présente loi ne s'applique pas aux droits des personnes concernées dans le cadre de procédures pendantes devant des tribunaux fédéraux ou cantonaux ou dans le cadre de procédures pendantes régies par le code de procédure pénale ou par la loi du 20 mars 1981 sur l'entraide pénale internationale, ni dans le cadre de la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ceux-ci sont régis par le droit de procédure applicable.

### Art. 2 Définitions

[1] Par données génétiques, on entend les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN.

[2] Par données biométriques, on entend les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique.

[3] Par profilage, on entend toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant la situation économique, la santé, les préférences personnelles, les intérêts, le comportement, la localisation ou les déplacements de cette personne.

[4] Par décision individuelle automatisée, on entend toute décision prise exclusivement sur la base d'un traitement de données personnelles automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

[5] Les données génétiques ou biométriques sont des données sensibles au sens de la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD).

[6] Le Préposé, au sens de la présente loi est celui institué par la LPrD.

[7] Par violation de la sécurité des données, on entend toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, qui entraîne la perte de données personnelles, leur modification, leur effacement ou leur destruction, ou encore leur divulgation ou un accès non autorisés. La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences ou qui fait preuve de négligence. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut aussi engendrer une violation de la personnalité, par exemple en entraînant la divulgation d'informations que la personne souhaitait garder secrètes.

# Titre II Obligations des organes traitant des données

## Art. 3 Devoir d'informer la personne concernée en cas de décision individuelle automatisée

[1] Le responsable du traitement informe la personne concernée de toute décision individuelle automatisée prise à son égard, avant la prise de cette décision; il qualifie cette décision comme telle.

[2] Si la personne concernée le demande, le responsable du traitement lui donne la possibilité de faire valoir son point de vue. La personne concernée peut exiger que la procédure appliquée lui soit communiquée et que la décision soit revue par une personne physique.

[3] L'alinéa 2 du présent article ne s'applique pas lorsque la personne concernée dispose d'une voie de droit contre la décision.

## Art. 4 Protection des données dès la conception et par défaut

[1] Les responsables du traitement sont tenus de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données et en particulier les principes fixés par la présente loi.

[2] Les mesures techniques et organisationnelles doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue, ainsi que du risque que le traitement des données en question présente pour les droits fondamentaux des personnes concernées.

[3] Les responsables du traitement sont tenus, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie.

## Art. 5 Principe de légalité

[1] Une base légale formelle est nécessaire pour fonder un mode de traitement susceptible de porter atteinte aux droits fondamentaux ou un profilage.

[2] Une base légale formelle n'est pas nécessaire si :

**a.** il existe un besoin de protection de la vie ou de l'intégrité corporelle de la personne concernée ou d'un tiers, ou :

**b.** la personne concernée a rendu ses données personnelles accessibles à tout un chacun, ou :

**c.** la personne concernée ne s'est pas opposée expressément au traitement.

## Art. 6 Registre des activités de traitement

[1] Les responsables du traitement tiennent un registre des activités de traitement.

[2] Les registres des responsables du traitement contiennent au moins les indications suivantes :

**a.** le nom du responsable du traitement;

**b.** la finalité du traitement;

**c.** une description des catégories des personnes concernées et des catégories des données personnelles traitées;

**d.** les catégories des destinataires;

**e.** la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour déterminer la durée de conservation;

**f.** dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données;

**g.** l'Etat tiers ou l'organisme international auquel des données personnelles sont communiquées ainsi que les garanties de protection des données personnelles prévues.

## Art. 7 Analyse d'impact relative à la protection des données personnelles

[1] Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux de la personne concernée, Le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitements semblables, il peut établir une analyse d'impact commune.

[2] L'existence d'un risque élevé dépend, en particulier lors de l'utilisation de nouvelles technologies, de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants :

**a.** le traitement de données sensibles ou de profils de la personnalité à grande échelle;

**b.** le profilage.

[3] L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger ceux-ci.

## Art. 8 Consultation du Préposé

[1] Le responsable du traitement consulte le Préposé, préalablement au traitement, lorsque l'analyse d'impact relative à la protection des données révèle que le traitement présenterait un risque élevé pour les droits fondamentaux de la personne concernée si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque.

[2] Le Préposé communique au responsable du traitement ses objections concernant le traitement envisagé dans un délai de deux mois. Ce délai peut être prolongé d'un mois, lorsqu'il s'agit d'un traitement de données complexe.

[3] Si le Préposé a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées.

## Art. 9 Annonce des violations de la sécurité des données

[1] Le responsable du traitement annonce dans les meilleurs délais au Préposé les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour les droits fondamentaux de la personne concernée.

[2] L'annonce doit au moins indiquer la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées pour y remédier.

[3] Le sous-traitant annonce dans les meilleurs délais au responsable du traitement tout cas de violation de la sécurité des données.

[4] Le responsable du traitement informe la personne concernée lorsque cela est nécessaire pour sa protection ou lorsque le Préposé l'exige.

[5] Le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer, dans les cas suivants :

**a.** les intérêts prépondérants d'un tiers l'exigent;

**b.** un intérêt public prépondérant, en particulier le maintien de la sûreté intérieure ou extérieure du canton ou de la Suisse, l'exige;

**c.** l'information de la personne concernée est susceptible de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire;

**d.** le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés;

**e.** l'information de la personne concernée est garantie de manière équivalente par une communication publique.

## Art. 10 Conseiller à la protection des données

[1] Les responsables du traitement désignent un conseiller à la protection des données. Ils peuvent désigner un conseiller commun.

[2] Le conseiller à la protection des données doit remplir les conditions suivantes:

**a.** il dispose des connaissances professionnelles nécessaires;

**b.** il n'exerce pas d'activités incompatibles avec ses tâches de conseiller à la protection des données.

[3] Le conseiller à la protection des données exerce notamment les tâches suivantes :

**a.** il conseille les responsables du traitement;

**b.** il promeut l'information et la formation des collaborateurs;

**c.** il concourt à l'application des prescriptions relatives à la protection des données et propose des mesures s'il apparaît que des prescriptions relatives à la protection des données ont été violées.

# Titre III Droits des personnes concernées

## Art. 11 Prétentions et procédure

[1] Quiconque a un intérêt légitime peut exiger du responsable du traitement :

**a.** qu'il s'abstienne de procéder à un traitement illicite;

**b.** qu'il supprime les effets d'un traitement illicite;

**c.** qu'il constate le caractère illicite d'un traitement.

[2] Le demandeur peut en particulier exiger que le responsable du traitement :

**a.** rectifie les données personnelles, les efface ou les détruise;

**b.** publie ou communique à des tiers sa décision concernant notamment la rectification, l'effacement ou la destruction des données, l'opposition à une communication ou la mention du caractère litigieux des données personnelles prévue à l'alinéa 4 du présent article.

[3] Au lieu d'effacer ou de détruire les données personnelles, le responsable du traitement limite le traitement dans les cas suivants:

**a.** l'exactitude des données est contestée par la personne concernée et leur exactitude ou inexactitude ne peut pas être établie;

**b.** des intérêts prépondérants d'un tiers l'exigent;

**c.** un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure du canton ou de la Suisse, l'exige;

**d.** l'effacement ou la destruction des données est susceptible de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire.

[4] Si l'exactitude ou l'inexactitude d'une donnée personnelle ne peut pas être établie, il ajoute à la donnée la mention de son caractère litigieux.

[5] La procédure est régie par la loi du 28 octobre 2008 sur la procédure administrative (LPA).

# Titre IV Surveillance

## Art. 12 Enquête du Préposé

[1] Le Préposé ouvre d'office ou sur dénonciation une enquête contre le responsable du traitement ou le sous-traitant si des indices font penser qu'un traitement de données personnelles pourrait être contraire à des dispositions de protection des données.

[2] Il peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance.

[3] Le responsable du traitement ou le sous-traitant fournit au Préposé tous les renseignements et les documents qui lui sont nécessaires pour l'enquête.

[4] Si la personne concernée est l'auteur de la dénonciation, le Préposé l'informe des suites données à celle-ci et du résultat d'une éventuelle enquête.

## Art. 13 Pouvoirs du Préposé

[1] Lorsque le responsable du traitement ou le sous-traitant ne respecte pas son obligation de collaborer, le Préposé peut, dans le cadre de la procédure d'enquête, ordonner notamment :

**a.** l'accès à tous les renseignements, documents, registres des activités et données personnelles nécessaires pour l'enquête;

**b.** l'accès aux locaux et aux installations;

**c.** l'audition de témoins;

**d.** des expertises.

[2] Il peut également ordonner des mesures provisionnelles pour la durée de l'enquête.

## Art. 14 Mesures administratives

[1] Si des dispositions de protection des données sont violées, le Préposé peut ordonner la mise en conformité, la suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles.

[2] Il peut suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux dispositions légales applicables en matière de communication de données personnelles à un Etat tiers ou à un organisme international.

[3] Lorsque le responsable du traitement ou le sous-traitant a pris, durant l'enquête, les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données, le Préposé peut se limiter à prononcer un avertissement.

[4] Les parties à la procédure d'enquête, y compris les responsables de traitement, ont qualité pour recourir, y compris contre les décisions sur l'effet suspensif ou les mesures provisionnelles.

# Titre V Assistance administrative

## Art. 15 Assistance administrative internationale

[1] Le Préposé peut échanger des informations ou des données personnelles avec une autorité d'un Etat Schengen chargée de la protection des données personnelles pour l'accomplissement de leurs tâches légales respectives en matière de protection des données, pour autant que les conditions suivantes soient réunies :

**a.** la réciprocité en matière d'assistance administrative est garantie;

**b.** les informations et les données personnelles échangées ne sont utilisées que dans le cadre de la procédure liée à la protection des données personnelles à la base de la demande d'assistance administrative;

**c.** l'autorité destinataire s'engage à ne pas divulguer les secrets professionnels, d'affaires ou de fabrication;

**d.** les informations et les données personnelles ne sont communiquées à des tiers qu'avec l'accord préalable de l'autorité qui les a transmises;

**e.** l'autorité destinataire s'engage à respecter les charges et les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations et les données personnelles.

[2] Pour motiver sa demande d'assistance administrative ou pour donner suite à une demande d'assistance administrative de l'autorité requérante, le Préposé peut communiquer notamment les indications suivantes :

**a.** le nom du service responsable du traitement, du sous-traitant ou de tout autre organe tiers participant au traitement;

**b.** les catégories de personnes concernées;

**c.** l'identité des personnes concernées lorsque sa communication est indispensable à l'accomplissement des tâches légales du Préposé ou d'une autorité d'un Etat Schengen chargée de la protection des données;

**d.** les données personnelles ou les catégories de données personnelles traitées;

**e.** les finalités des traitements;

**f.** les destinataires ou les catégories de destinataires;

**g.** les mesures techniques et organisationnelles.

[3] Avant de transmettre à une autorité d'un Etat Schengen chargée de la protection des données des informations susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires, il informe les personnes détentrices de ces secrets et les invite à prendre position, à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés.

# Titre VI Dispositions supplétives et transitoires

## Art. 16 Dispositions supplétives

[1] A défaut de disposition spéciale prévue par la présente loi, la loi cantonale sur la protection des données personnelles (LPrD) s'applique; l'applicabilité d'autres lois est réservée.

[2] La loi sur la procédure administrative (LPA) s'applique en outre spécifiquement à la procédure à suivre concernant l'application des art. 11 à 14 de la présente loi.

## Art. 17 Exécution et entrée en vigueur

[1] Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a, de la Constitution cantonale et en fixera, par voie d'arrêté, l'entrée en vigueur.

# PROJET DE LOI
# modifiant celle du 11 septembre 2007 sur la protection des données personnelles du 6 juillet 2022

LE GRAND CONSEIL DU CANTON DE VAUD

*décrète*

***Article Premier***

[1] La loi du 11 septembre 2007 sur la protection des données personnelles est modifiée comme il suit :

**Art. 3 Champ d'application**

[1] La présente loi s'applique à tout traitement de données des personnes physiques ou morales.

[2] Sont soumis à la présente loi les entités suivantes :

**a.** le Grand Conseil ;

**b.** le Conseil d'Etat et son administration ;

**c.** l'Ordre judiciaire et son administration ;

**cbis.** la Cour des comptes ;

**Art. 3 Sans changement**

[1] Sans changement.

[2] Sans changement.

**a.** Sans changement.

**b.** Sans changement.

**c.** Sans changement.

**cbis.** Sans changement.

**d.** les communes, ainsi que les ententes, associations, fédérations, fractions et agglomérations de communes ;

**e.** les personnes physiques et morales auxquelles le canton ou une commune confie des tâches publiques, dans l'exécution desdites tâches.

[3] La présente loi ne s'applique pas :

**a.** aux délibérations du Grand Conseil et des conseils généraux et communaux ;

**b.** aux procédures civiles, pénales ou administratives ;

**c.** aux données personnelles traitées en application de la loi fédérale sur le renseignement et de l'article 2, alinéa 1 de la loi sur les dossiers de police judiciaire.

**d.** Sans changement.

**e.** Sans changement.

[3] Sans changement.

**a.** Sans changement.

**b.** Sans changement.

**c.** aux données personnelles traitées en application de la loi fédérale sur le renseignement.

### *Art. 2*

[1] Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a, de la Constitution cantonale et en fixera, par voie d'arrêté, l'entrée en vigueur.

# PROJET DE LOI
# modifiant celle du 1 décembre 1980 sur les dossiers de police judiciaire du 6 juillet 2022

LE GRAND CONSEIL DU CANTON DE VAUD

*décrète*

***Article Premier***

[1] La loi du 1 décembre 1980 sur les dossiers de police judiciaire est modifiée comme il suit :

| | |
|---|---|
| **Art. 1 Définition** | **Art. 1 Sans changement** |
| [1] Sont considérées comme dossiers de police judiciaire toutes les informations personnelles conservées par la police et relatives à un crime, un délit ou une contravention relevant du droit pénal fédéral, exception faite des condamnations portées au registre des contraventions de circulation. | [1] Sont considérées comme dossiers de police judiciaire toutes les informations personnelles conservées par la police et relatives à un crime, un délit ou une contravention relevant du droit pénal fédéral, cantonal ou communal. |
| [2] Les dossiers comprennent les documents littéraux ou photographiques (dossiers proprement dits) et les fichiers, quel que soit leur support matériel. | [2] Les dossiers comprennent les documents littéraux ou d'imagerie (dossiers proprement dits) et les fichiers, quel que soit leur support matériel. |

## Art. 2 Contenu des dossiers

[1] Seules les informations utiles à la prévention, la recherche et la répression des infractions peuvent être enregistrées.

[2] Il est notamment interdit de réunir et de conserver des informations sur les convictions politiques, morales ou religieuses des individus, à moins que celles-ci ne soient en relation étroite avec un crime ou un délit.

[3] Les données non pertinentes ou inadéquates doivent être radiées.

## Art. 8 Modalités

[1] Le droit d'accès est strictement limité aux besoins du service ou de la procédure de renseignements ou de rectification. Les dossiers sont consultés sur place, sous réserve des exceptions consenties par le commandement de la police cantonale.

[2] Aucun document tiré directement d'un dossier ni aucune fiche ne peuvent être emportés.

[3] Les photocopies sont interdites, sauf autorisation expresse du commandement de la police cantonale.

## Art. 8a Droit aux renseignements

[1] Toute personne peut demander des renseignements sur les données personnelles la concernant qui sont contenues dans les dossiers de police judiciaire.

## Art. 2 Sans changement

[1] Sans changement.

[2] Il est notamment interdit de réunir et de conserver des informations sur les convictions politiques, morales, religieuses ou concernant l'orientation sexuelle des individus, à moins que celles-ci ne soient en relation étroite avec un crime ou un délit.

[3] Sans changement.

## Art. 8 Sans changement

[1] Le droit d'accès est strictement limité aux besoins du service ou de la procédure de renseignements, de rectification ou de suppression. Les dossiers sont consultés sur place, sous réserve des exceptions consenties par le commandement de la police cantonale.

[2] Sans changement.

[3] Sans changement.

## Art. 8a Droit aux renseignements ou à la constatation d'un traitement illicite de donnés

[1] Sans changement.

| | |
|---|---|
| | [1a] Toute personne peut demander la constatation du caractère illicite d'un traitement de données la concernant. |
| [2] Le droit d'obtenir des renseignements peut être limité, suspendu ou refusé si un intérêt public prépondérant l'exige. Il en va de même si la communication des renseignements est contraire à des intérêts prépondérants ou légitimes de tiers ou de la personne concernée elle-même. | [2] Sans changement. |
| [3] Les dispositions du Code de procédure pénale sur l'enquête sont réservées. | [3] Sans changement. |
| | **Art. 8b Sans changement** |
| | [1] Hors procédure pénale, les demandes de renseignements sur les données personnelles et de constatation du caractère illicite d'un traitement de données sont traitées par un juge cantonal (ci-après: le juge) désigné à cet effet au début de chaque législature par le Tribunal cantonal. |
| **Art. 8c Procédure** | **Art. 8c Sans changement** |
| [1] La demande de renseignements est adressée au juge. | [1] La demande de renseignements sur les données personnelles ou de constatation du caractère illicite d'un traitement de données est adressée au juge. |
| [2] Le requérant doit justifier de son identité par la production d'une pièce de légitimation officielle. | [2] Sans changement. |
| [3] A l'appui de sa demande, le requérant doit rendre vraisemblable que des renseignements personnels à son sujet sont susceptibles de porter atteinte à sa liberté personnelle. A défaut, le juge pourra écarter préjudiciellement la demande. | [3] Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le juge peut: |

**a.** soit exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder à la communication ou prendre les mesures demandées;

**b.** soit refuser de donner suite à la demande. Il incombe au juge de démontrer le caractère manifestement infondé ou excessif de la demande.

[4] Si les données personnelles ont été communiquées à la police par des autorités de poursuite ou des organes de police d'autres cantons ou par la Confédération, le juge peut transmettre la requête pour décision à ces autorités ou organes.

[4] Sans changement.

[5] Le juge communique par écrit sa décision à la personne qui a demandé des renseignements et à la police. En cas d'acceptation, il lui fait transmettre par écrit les renseignements personnels qui la concernent. En cas de refus, il en indique brièvement les motifs. Sa décision est définitive.

[5] Le juge communique par écrit sa décision à la personne qui a demandé des renseignements et à la police. En cas de refus, il en indique brièvement les motifs.

[6] La décision du juge peut faire l'objet d'un recours au Tribunal cantonal.

**Art. 8d Droit de rectification**

[1] Celui qui apprend qu'une information inexacte le concernant figure dans un dossier de police judiciaire peut en demander la rectification.

[2] L'autorité compétente et la procédure sont celles prévues aux articles 8b et 8c.

[3] La charge de prouver au juge l'exactitude des données enregistrées incombe à la police.

**Art. 8d Droit de rectification ou de suppression**

[1] Celui qui apprend qu'une information inexacte le concernant figure dans un dossier de police judiciaire peut en demander la rectification ou la suppression.

[2] Sans changement.

[3] Sans changement.

[4] Le juge fait rectifier ou supprimer les données qui s'avèrent inexactes ou incomplètes auprès de tous les destinataires connus.

[5] Lorsque ni l'exactitude d'une donnée ni son inexactitude ne peuvent être établies, il en sera fait mention au dossier.

[6] Le juge renseigne le requérant sur les mesures qu'il a ordonnées. Sa décision est définitive.

[4] Sans changement.

[5] Sans changement.

[6] Le juge renseigne le requérant sur les mesures qu'il a ordonnées.

**Art. 8g Droit supplétif**

[1] La loi sur la protection des données et la loi sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal s'appliquent à titre supplétif.

***Art. 2***

[1] Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a, de la Constitution cantonale et en fixera, par voie d'arrêté, l'entrée en vigueur.