Session ordinaire 2019-2020

MW/PR

P.V. SID 15
P.V. J 33

Commission de la Sécurité intérieure et de la Défense

Commission de la Justice

Procès-verbal de la réunion du 28 mai 2020

Ordre du jour :

1. Élaboration d'une base légale spécifique pour les traitements de données à caractère personnel effectués par la Police grand-ducale

   - Continuation des travaux

2. Mise en œuvre des recommandations comprises dans les études effectuées par la CNPD et l'IGP concernant les traitements de données à caractère personnel effectués par la Police grand-ducale

   - Continuation des travaux

*

Présents : Mme Diane Adehm, Mme Semiray Ahmedova, Mme Nancy Arendt épouse Kemp, M. Carlo Back, M. Dan Biancalana, Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, M. Max Hahn, M. Jean-Marie Halsdorf, Mme Cécile Hemmen, M. Fernand Kartheiser, M. Claude Lamberty, M. Georges Mischo, membres de la Commission de la Sécurité intérieure et de la Défense

M. Marc Baum, observateur délégué

Mme Diane Adehm, M. Guy Arendt, M. François Benoy, M. Dan Biancalana, Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, Mme Carole Hartmann, Mme Cécile Hemmen, M. Pim Knaff, M. Charles Margue, M. Laurent Mosar, M. Roy Reding, M. Gilles Roth, membres de la Commission de la Justice

M. Marc Baum, observateur délégué
Mme Viviane Reding, observatrice

M. François Bausch, Ministre de la Sécurité intérieure
M. Henri Kox, Ministre délégué à la Sécurité intérieure
Mme Sam Tanson, Ministre de la Justice

Mme Béatrice Abondio, Mme Barbara Ujlaki, du Ministère de la Sécurité intérieure

Police grand-ducale :

M. Philippe Schrantz, Directeur général, M. Jeff Neuens, Direction générale, Mme Lydie May, Data Protection Officer (DPO)

Inspection générale de la Police (IGP) :

Mme Monique Stirn, Inspecteur général, M. Vincent Fally, Inspecteur général adjoint

M. Gil Goebbels, M. Bob Lallemang, du Ministère de la Justice

M. Vincent Wellens, Nauta*Dutilh*

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : M. Gusty Graas, membre de la Commission de la Sécurité intérieure et de la Défense

Mme Octavie Modert, membre de la Commission de la Justice

*

Présidence : Mme Stéphanie Empain, Présidente de la Commission de la Sécurité intérieure et de la Défense, M. Charles Margue, Président de la Commission de la Justice

*

Monsieur le Ministre de la Sécurité intérieure informe les députés que la présentation de l'état actuel du texte de loi inclut deux propositions relatives à l'archivage dans le domaine du fichier central de la Police, répondant respectivement par l'affirmative et par la négative à la question de savoir si un archivage sera encore fait à l'avenir. S'agissant de la première, il est proposé de maintenir un archivage pour la raison que les délais de conservation des données au fichier central se trouveraient ainsi considérablement réduits.

La version actuelle du texte sera transmise dans les deux prochains jours aux députés qui pourront remettre dans les semaines à venir leurs questions, observations et suggestions aux auteurs. Une prochaine réunion sera consacrée à la discussion de la nouvelle version qui sera finalisée ensuite pour être soumise au Conseil de gouvernement fin juillet.

Monsieur le Ministre fait distribuer plusieurs documents informant sur l'avancement des travaux, dont un tableau actualisé relatif à la mise en œuvre des recommandations de la CNPD et de l'IGP concernant les traitements de données à caractère personnel effectués par la Police. Quant aux avertissements taxés, le texte opère une distinction claire entre les volets administratif et judiciaire.

Au moyen d'un document PowerPoint (cf. annexe), M. Vincent Wellens présente les changements opérés depuis la présentation faite le 5 mars 2020.

La loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, transposant 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, reste évidemment la loi-cadre.

Les dispositions ajoutées entretemps au texte en cours d'élaboration précisent ce cadre sur certains points. Elles seront insérées dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale au titre relatif à la protection des données (annexe p. 2). L'article 43-1 contient les dispositions communes qui s'appliquent à tous les fichiers opérationnels de la Police, donc les fichiers qui tombent dans le champ d'application de la loi du 1er août 2018 précitée. La sous-catégorie des fichiers particuliers sera régie par l'article 43-1 ; afin de ne pas surcharger la loi sur la Police grand-ducale, il est renoncé à la création d'une catégorie à part dans la loi. La protection des données étant une matière réservée à la loi, certains points sont redirigés vers la loi, la voie du règlement grand-ducal étant abandonnée, tandis que d'autres aspects pourront être réglés de manière interne par la Police. L'article 43-2 contient des dispositions qui traitent plus spécifiquement de la refonte du fichier central.

La philosophie de l'avant-projet de loi (annexe p. 3) consiste à tenir en équilibre l'exigence d'un encadrement plus strict de certains fichiers au niveau légal et l'efficacité policière, ainsi que la responsabilisation de la Police. Le texte tient compte des points les plus critiques soulevés par l'IGP[1] et la CNPD[2] dans leurs avis respectifs, à savoir la gestion de l'accès aux fichiers, les délais de conservation des données, la protection des mineurs et la précision des finalités. Les autres aspects sont réglés au niveau de la Police, ce qui est parfaitement en phase avec le nouveau paradigme en matière de protection des données, à savoir qu'il y a un responsable du traitement, lequel doit veiller à la conformité du traitement des données à la loi.

Comme déjà mentionné, le recours au règlement grand-ducal est évité pour des raisons de constitutionnalité et pour rompre avec la situation en vigueur sur base de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État. En vertu de la loi précitée du 2 août 2002, un règlement grand-ducal devait être pris pour chaque fichier de la Police.

Éviter les redondances avec le cadre légal existant s'est révélé être un exercice difficile (annexe p. 4). La loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale précitée est une transposition fidèle de la directive (UE) 2016/680. Elle contient tous les principes de base en matière de protection des données. En outre, elle distingue entre les personnes concernées, de même qu'entre les faits et les appréciations personnelles, et elle prévoit dans quel cas la CNPD doit être impliquée. L'application de la loi précitée du 1er août 2018 donnant déjà la réponse à une multitude de questions, le but poursuivi consiste à se concentrer sur les points les plus critiques.

Le transfert de données à d'autres autorités est un autre point qu'on a déjà envisagé de reprendre dans le nouveau dispositif législatif. Le dispositif existant est la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en

[1] Inspection générale de la Police
[2] Commission nationale pour la protection des données

matière policière et portant : 1) transposition de la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ; 2) mise en œuvre de certaines dispositions de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

Dispositions applicables à tous les fichiers (annexe p. 5-7)
L'objet et la portée ont été clarifiés. Plus précisément, le champ d'application a été synchronisé avec celui de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale précitée, qui s'applique aussi aux traitements de données à caractère personnel effectués par la Police, tant pour le domaine de la police judiciaire que pour celui de la police administrative. En outre, la même loi précitée du 1er août 2018 prévoit qu'elle « s'applique également aux traitements de données à caractère personnel effectués :
a) par la Police grand-ducale dans l'exécution de missions à des fins autres que celles visées au paragraphe 1er et prévues par des lois spéciales, » (article 1er, paragraphe 2, a) ».
Ce qui est donc exclu du champ d'application sont les fichiers liés aux fonctions internes (fichiers Ressources humaines, etc.) et les matières régies par des lois spécifiques existantes (par exemple empreintes digitales, ADN).

Il est important de préciser que la Police en tant qu'entité (au lieu de son Directeur général) est le responsable de traitement et de suivre la même ligne dans d'autres textes de loi.

Un paragraphe a été inséré sur les données qui relèvent de catégories particulières, telles les données de santé, les données relatives à la religion, etc., précisant bien quand la Police peut faire un traitement de ces données. La loi précitée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale contient une disposition relative à ces catégories particulières, à savoir l'article 9 :
« **Art. 9. Traitement portant sur des catégories particulières de données à caractère personnel**
Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont autorisés uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :
a) lorsqu'ils sont autorisés par le droit de l'Union européenne ou en application de la présente loi ou d'une autre disposition du droit luxembourgeois ;
b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou
c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. ».

Une garantie supplémentaire a été introduite en phase avec l'un des considérants de la directive, à savoir que des données comme celles relatives à la santé ne peuvent pas être traitées de manière isolée, mais doivent toujours l'être en rapport avec d'autres données.[3]

En raison de la panoplie de fichiers, il est impossible d'inscrire dans la loi pour chaque fichier une durée de conservation des données. L'option a été choisie de préciser dans la loi que le

[3] Directive (UE) 2016/680, considérant 24 : « Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. (…) »

délai de conservation s'appliquant au fichier central est le délai maximal de conservation, sauf si une disposition légale spécifique prévoit une durée plus longue. La Police doit ensuite déterminer un délai de conservation par type de fichier qui ne dépasse pas le délai maximal.

Les critères de base pour les règles d'accès sont précisés dans la loi. Sur cette base, la Police définira son concept pour les règles d'accès à chaque fichier. Ces critères sont les suivants (annexe p. 7) : le détail des informations, les motifs d'accès (ces motifs différant suivant le type de mission (police judiciaire/police administrative), le type de traitement (qui peut inscrire une donnée dans un fichier et qui peut la modifier ?), l'appartenance à un service déterminé (ce critère étant lié à celui des motifs d'accès), la protection des mineurs qui suit des règles spécifiques, l'état de validation d'une information (tant que l'information n'est pas validée par le supérieur hiérarchique, l'accès est restreint).

S'agissant de la possibilité d'appliquer des sanctions pénales en cas de violation intentionnelle des règles d'accès, un rappel des articles 509-1 à 509-7 du Code pénal est prévu dans la loi. En outre, l'exposé des motifs du projet de loi indiquera la jurisprudence, selon laquelle ces dispositions pénales s'appliquent aussi au policier qui a accès, mais qui en abuse par un détournement de l'information.

Dispositions applicables au fichier central (annexe p. 9 et 10)
Les finalités sont :
- vérification des antécédents ; aide aux contrôles effectués ; les auteurs se sont inspirés ici de la loi belge, à laquelle fait référence la CNPD dans son avis du 13 septembre 2019 sur le fichier central de la Police ;

[Extrait de l'avis de la CNPD :
« En Belgique, la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel met en œuvre le RGPD et transpose la Directive en droit national. Cette loi prévoit également la nécessité d'une base légale spécifique à savoir un texte légal ou réglementaire encadrant les traitements de données à caractère personnel en matière pénale. Dans la lignée du législateur français, le législateur belge dote les fichiers de la police de bases légales spécifiques. En effet, la loi sur la fonction de police dispose que « lorsque l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations visées à l'article 44/1 de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle [..] ». La loi encadre trois types de fichiers à savoir « la Banque de données Nationale Générale », « les banques de données de base », « les banques de données particulières ». La loi belge précise également les finalités de ces trois types de banques de données. A titre d'exemple, la Banque de données Nationale Générale est utilisée par les services de police belge pour exercer leurs missions afin de permettre : « l'identification des personnes visées à l'article 44/5 , paragraphe 1er et 3 ; l'identification des personnes ayant accès à la B.N.G. ; la coordination et le croisement des données à caractère personnel et informations policières ; la vérification au niveau national des antécédents de police administrative et de police judiciaire ; l'aide aux contrôles effectués par les services de police par l'indication des mesures à prendre soit sur la base d'une décision des autorités de police administrative ou des autorités de police judiciaire compétentes, soit en fonction de l'existence des antécédents de police administrative ou de police judiciaire ; l'appui à la définition et à la réalisation de la politique policière et de sécurité ».]

- définir une politique de sécurité intérieure à des fins de statistiques ;
- faire des analyses criminelles opérationnelles, permettant à la Police de faire des recherches, dans le cadre d'une enquête, sur deux dossiers différents pour voir les rapports ;
- les données en rapport avec les avertissements taxés (AT) réglés ne figureront pas au fichier central.

Quant aux catégories de personnes, dont les données à caractère personnel seront traitées au niveau du fichier central, il s'agit pour le domaine de la police administrative et celui des autres missions légales de la Police des personnes directement concernées par les mesures et rapports. Dans le domaine de la police judiciaire, on distingue trois catégories : en premier

lieu, il s'agit des personnes suspectes, condamnées, recherchées, etc. ; ensuite, les victimes et témoins – ici, une consultation pour motif non-judiciaire n'est pas possible ; enfin la catégorie des personnes « données douces », où une consultation pour motif non-judiciaire n'est pas non plus possible et en plus, des règles spécifiques d'inscription et d'accès seront à respecter.

Il y aura deux catégories de données : la partie « informations principales », énumérées de manière exhaustive dans la loi, et la partie « documents », cette dernière se traduisant plutôt par un lien qui va apparaître dans un dossier vers un document, avec des droits d'accès différents. Une énumération exhaustive et précise n'est pas possible pour la partie « documents » (procès-verbaux, rapports) ; en vertu du Code de procédure pénale, l'agent de police doit constater tout ce qui peut être utile dans le rapport. Les informations principales sont évidemment susceptibles de se trouver aussi dans les rapports et procès-verbaux.

Concernant les relations avec d'autres fichiers, il est tenu compte du secret d'enquête, ce qui implique que, dans le domaine des missions de police judiciaire, des données peuvent être introduites dans le fichier central uniquement si l'enquête est terminée ou s'il y a une autorisation des autorités judiciaires. Pour le reste, la loi précitée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale prévoit l'utilisation des données à d'autres finalités.

En ce qui concerne la durée de conservation et d'archivage (annexe p. 11), deux options sont présentées, comme déjà annoncé par Monsieur le Ministre. L'option A (sans archivage) propose, dans le domaine de la police judiciaire, un délai de conservation provisoire de 10 ans en matière de crimes et délits et de 3 ans dans celle des contraventions. Avant l'expiration du délai, la Police demande aux autorités judiciaires s'il faut prolonger le délai. Les données sont supprimées en cas d'acquittement de la personne, en cas de sa réhabilitation après condamnation et en cas de prescription de l'action publique. Les autorités judiciaires sont libres de procéder d'un archivage de leur côté.
Dans le domaine de la police administrative et des autres missions légales de la Police, un délai maximal de 10 ans est proposé, avec la possibilité de prévoir un délai plus court pour des rapports particuliers.

L'option B est celle prévoyant un archivage, mais uniquement dans le domaine de la police judiciaire. L'archivage, pour lequel une durée de 30 ans est prévue, ne consiste pas à transmettre les données dans un autre système, des archives à part, mais par une partie passive accessible de manière très restreinte, précisément pour des fins judiciaires avec l'accord du Procureur général d'État.

Madame la Ministre de la Justice indique que la discussion de l'option A avec les autorités judiciaires est encore en cours. Avant de prendre position, il serait utile pour les députés de s'informer auprès des autorités judiciaires sur les implications pour la Justice. En effet, comme il n'existe pas encore de fichier central judiciaire, il est procédé dans les dossiers sous forme de note avec renvoi à l'archivage de la Police. En cas de besoin, les autorités judiciaires demandent les données nécessaires auprès de la Police.

Monsieur le Ministre de la Sécurité intérieure fait remarquer que l'option sans archivage a été élaborée sur demande parlementaire.

Discussion

Le groupe politique CSV salue les efforts réalisés par les auteurs, sachant que la discussion ne se fera ultérieurement qu'en disposant du texte de loi. M. Gilles Roth constate qu'il est question de l'acquittement, mais pas du non-lieu, à moins que celui-ci ne soit assimilé à

l'acquittement au niveau de l'instruction, et pas non plus du classement sans suite. M. Roth souhaitant connaître la manière de procéder en cas d'un non-lieu prononcé par une juridiction d'instruction, en se trouvant dans l'option A (sans aucun archivage), M. Wellens fait savoir qu'il est effectivement prévu de l'assimiler à un acquittement, des détails restant encore à clarifier avec la Justice concernant la conservation/l'archivage. Pour M. Roth, il n'existe pas de besoin de clarification, puisque selon une jurisprudence constante, un non-lieu, dès que l'action publique est prescrite, équivaut à un acquittement, ce qui signifie que les données sont à supprimer.

En ce qui concerne l'option A (sans aucun archivage), M. Roth s'étonne du stockage des données pendant 10 ans pour les crimes et délits et pendant 3 ans pour les contraventions, c'est-à-dire d'une durée de stockage qui dépasse le délai de prescription de l'action publique des délits (5 ans) et des contraventions (1 an).

Selon M. Vincent Wellens, il s'agit d'une période de conservation provisoire. En effet, il est prévu de rendre le retour d'informations des autorités judiciaires vers la Police plus fluide. Si, par exemple, un acquittement intervient entretemps, les données sont supprimées avant, au lieu d'être conservées pendant 10 ans.

M. Roth insiste sur la nécessité de la suppression immédiate des données en cas de non-lieu et d'acquittement. Un stockage qui va en outre au-delà du délai de prescription de l'action publique ne se justifie pas et est en plus contraire aux droits de l'Homme. En cas de classement sans suite, la conservation des données peut se discuter, comme le parquet peut revenir sur sa décision et engager des poursuites ; toutefois, si les faits sont prescrits, cela n'est plus possible et il n'y a plus de raison pour un stockage.

Il sera tenu compte de ce point, M. Wellens indiquant que le concept a aussi été élaboré avec la Police et le comité de suivi, où est représentée notamment la CNPD.

En outre, M. Roth croyait qu'un accord avait été trouvé pour réintroduire des sanctions pénales telles que prévues par la loi précitée du 2 août 2002, au lieu de renvoyer simplement aux articles 509-1 à 509-7 du Code pénal. Ainsi, l'article 509-1 concerne une intrusion frauduleuse dans un système[4] ; par contre, une simple manipulation ou négligence, par exemple le fait de laisser traîner le mot de passe, ne seraient plus sanctionnées pénalement, alors que la loi précitée du 2 août 2002 énumère dans son chapitre V une série de règles relatives à la confidentialité ou la sécurité des traitements et prévoit les sanctions pour violation de ces règles. Un abandon de ces infractions et sanctions serait incompréhensible.

Madame la Ministre de la Justice fait savoir que la veille à la Commission de la Justice a été discutée de manière générale la question de savoir si, en matière de protection des données, les sanctions administratives devraient être remplacées par des sanctions pénales.

Posant la question de savoir si des sanctions pénales sont à inscrire dans la future loi sur les fichiers de la Police, Monsieur le Ministre suggère que, sur base des réflexions faites, une proposition de texte sera élaborée.

---

[4] « **Art. 509-1.**
(L. 14 août 2000) Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros. »

Enfin, un point non abordé est celui de l'information des personnes dont les données sont stockées. Or, l'orateur considère cette information comme absolument nécessaire. En cas, notamment, de jugement ayant force de chose jugée ou d'une instruction clôturée sans suite, les données sont à supprimer et les personnes concernées doivent en être informées. Le maintien des données irait à l'encontre des principes de droit. L'orateur renvoie dans ce contexte à l'avis précité de la CNPD sur le fichier central de la Police et aux législations belge et française.

En complément des remarques faites par M. Roth, M. Laurent Mosar (CSV), exprimant ses remerciements pour le travail réalisé, constate l'absence d'un chapitre relatif à la suppression des données. Il s'agit d'un sujet d'une importance telle qu'il mérite d'être traité séparément, en établissant des règles précises.

De même, au-delà de la voie passant par la CNPD, des précisions manquent quant à l'accès des citoyens au fichier, en particulier pour vérifier si les données qui les concernent sont effectivement supprimées.

De la part du Ministère de la Sécurité intérieure, il est rappelé que le droit d'accès prévu par l'article 13 de la loi précitée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale permet aux citoyens de savoir si un traitement de données les concernant existe auprès de la Police, de même que d'accéder à leurs données. La procédure est déterminée de manière interne ; si une mention peut bien en être faite dans la loi, une inscription de la procédure complète dans la loi n'est toutefois pas indiquée.

Un volet très important est celui de la coopération nationale, notamment entre la Police, les autorités judiciaires et l'Administration des douanes et accises. Pour M. Mosar, cette coopération, plus précisément l'échange de données, a besoin d'être clarifiée de manière générale.

Confirmant que l'Administration des douanes et accises a accès au fichier « Stupéfiants », Monsieur le Ministre préférerait en général que les données soient demandées à la Police au lieu de disposer d'un accès direct au fichier. Si un tel accès est justifié pour les autorités judiciaires, les autres administrations ne devraient pas en disposer.

Selon Madame la Ministre de la Justice, il convient d'examiner dans quelle mesure la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière[5] règle cette question.

M. Mosar souligne que le même problème se présente en matière d'accès aux données de santé.

Rappelant que le groupe politique CSV plaide pour l'abandon de l'archivage, M. Mosar salue néanmoins la présentation de deux options, ce qui permet de faire une comparaison pour trouver une solution adéquate.

À la demande de M. Mosar d'être informé sur l'état actuel de la procédure relative aux AT, Monsieur le Ministre de la Sécurité intérieure se réfère à la note ministérielle distribuée au

[5] Loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière et portant :
1) transposition de la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ;
2) mise en œuvre de certaines dispositions de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière

cours de la présente réunion aux députés[6]. Depuis le début du processus de dépersonnalisation dès leur acquittement, à savoir depuis le 11 avril 2020, 682 716 AT en matière d'arrêt, de stationnement et de parcage ont été dépersonnalisés, de même que 472 688 AT en matière de CSA[7].

En réponse à une question de M. Mosar, Monsieur le Directeur général de la Police rassure que les agents municipaux n'avaient pas d'accès au fichier AT, mais au dixième AT impayé d'une personne, ils en recevaient l'information, afin de pouvoir appeler la police pour faire donner une amende.

Mme Stéphanie Empain (déi gréng) souhaitant savoir si la manière technique de vérification de l'état de la procédure auprès des autorités judiciaires (option A – Police judiciaire) est déjà déterminée, M. Wellens répond par la négative.

Mme Viviane Reding (CSV) s'intéresse au volet de la coopération internationale, en songeant notamment à Europol et Interpol, plus précisément à l'application des règles déterminées au niveau national dans l'échange international (impact des règles relatives à la prescription, à la suppression de données, etc. sur les informations demandées par ou reçues d'autres pays).

Un représentant de la Police souligne qu'il n'existe pas d'accès direct d'une banque de données internationale sur le fichier central de la Police. Par le passé, les signalements par Interpol (Europol n'existant pas encore ; correspondant aujourd'hui au mandat d'arrêt européen) étaient repris dans la partie « Signalétique » du fichier central, de sorte qu'un policier ayant affaire à une personne recherchée au niveau international en avait tout de suite connaissance. Aujourd'hui, la Police dispose de l'accès direct aux banques de données Interpol et Schengen ; le fichier central contient le volet national des signalements et les informations relatives aux mandats d'arrêt européens. Concernant la prescription, si une demande d'information est adressée par une autorité étrangère à la Police et qu'il y a eu suppression ou archivage, la Police ne dispose évidemment plus des données. En cas d'archivage, il faut examiner si une demande d'accès à la partie « Archives » auprès des autorités judiciaires est utile ou non.

*

Divers

Revenant au débat de consultation qui vient d'avoir lieu à la Chambre des Députés sur la réforme de la Police, M. Laurent Mosar (CSV) se réfère aux propos de Monsieur le Ministre qui s'est déclaré disposé à discuter sur une adaptation législative, en ce qui concerne les outils dont dispose la Police pour ses interventions. Il s'avère que la situation au centre-ville et en particulier au quartier de la gare est grave, et aussi insatisfaisante pour la Police qui est limitée dans ses moyens d'action. L'orateur demande que le sujet soit d'urgence mis à l'ordre du jour d'une réunion des deux commissions, à laquelle devraient participer aussi des représentants des autorités judiciaires.

Monsieur le Ministre précise que la loi est effectivement à préciser, pour ce qui est des personnes qui bloquent les entrées d'habitations ; les travaux sont en cours. S'agissant d'autres actions, comme faire un barbecue dans la zone piétonnière, la législation actuelle interdit ces actions et prévoit des punitions.

À son tour, Madame la Ministre de la Justice est également prête à rediscuter ce sujet.

[6] Note du 28 mai 2020 – « Objet : Avertissements taxés – Continuation des travaux »
[7] Contrôle Sanction Automatisé (radars automatiques)

Le Secrétaire-administrateur,
Marianne Weycker

La Présidente de la Commission de la Sécurité intérieure et de la Défense,
Stéphanie Empain

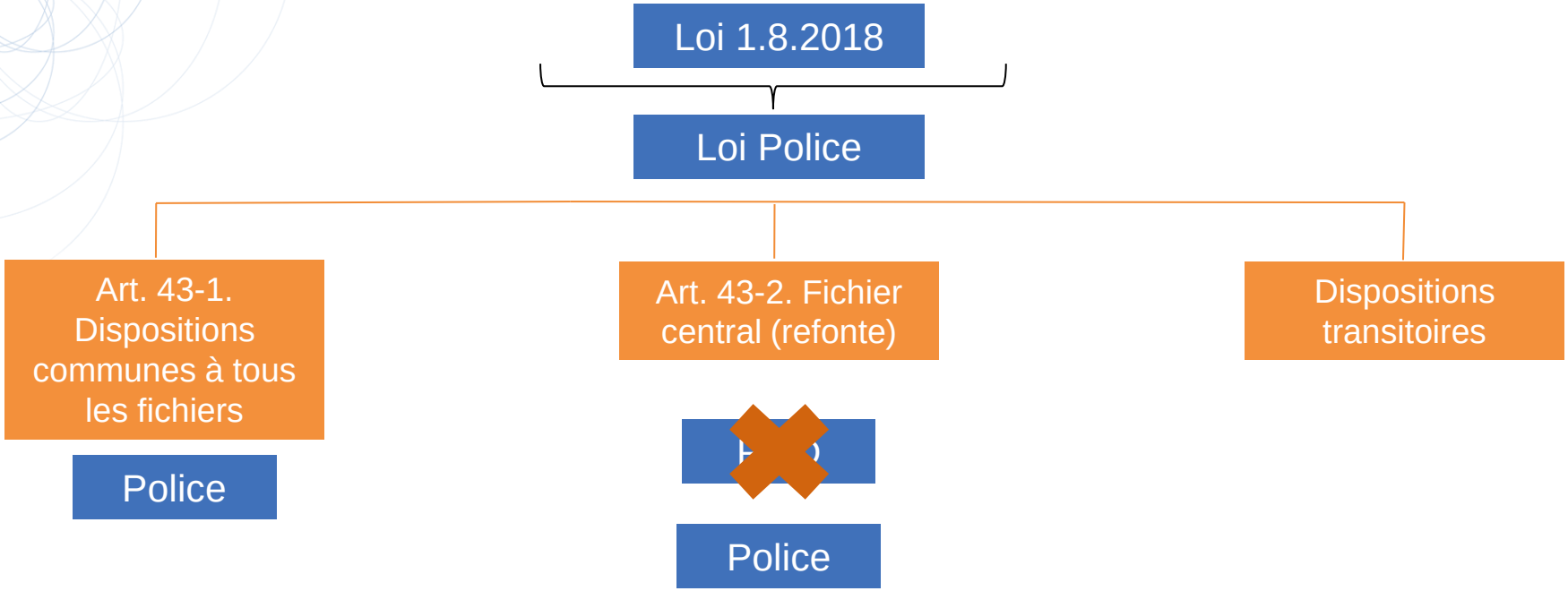
Le Président de la Commission de la Justice,
Charles Margue

Annexe

Présentation de l'avant-projet de loi sur les fichiers de la Police

28 mai 2020 – Chambre des députés : commission de la Sécurité intérieure et de la Défense

Proposition de structure du nouvel encadrement



Exposé des motifs : pourquoi cette structure et sa conformité à la Constitution – dans l'état actuel la base légale (et valable) est la Loi du 1er août 2018 + mesures internes de la Police: la structure envisagée ne fait que renforcer les garanties existantes tant sur le contenu que sur le plan formel

Philopsophie de l'APL (1)

- Equilibre entre encadrement plus strict >< efficacité policière et responsabilisation de la Police
  - Encadrer dans la nouvelle loi principalement les points les plus critiques identifiés dans les avis de la CNPD et de l'IGP :
    - Gestion des accès fichiers
    - Délais de conservation fichiers
    - Protection mineurs
    - Précision des finalités
  - Les autres aspects sont réglés au niveau de la Police = nouveau paradigme en protection des données
  - Eviter le recours à des RGD pour des raisons de constitutionnalité + rupture avec la Loi 2.8.2002

Philopsophie de l'APL (2)

- Eviter des redondances avec le cadre légal existant
  - Loi 1.8.2018 (Dir. (UE) 2016/680)
    - Principes de base : limitation finalité, minimisation de données (~accès + conservation)
    - Distinction personnes concernées (suspect, condamné, victime, …)
    - Distinction faits >< appréciations personnelles
    - Droits des personnes concernées
    - Analyse d'impact protection des données et consultation CNPD
    - …
  - Loi 22.2.2018 (échanges de données en matière policière)
    - Coopération internationale
    - Coopération nationale

1 Les dispositions applicables à tous les fichiers

2 Les dispositions applicables au fichier central

- Objet et portée : tous les fichiers liés aux activités de la Police
  - à l'exclusion des fichiers liés aux fonctions internes, comme les fichiers RH
  - sauf s'il y a des règles différentes adoptées par une loi spécifique (par ex. ADN)
- Police : responsable de traitement
- Données particulières (santé, réligion, orientation sexuelle, race, …) :
  - Renforcer la base légale + garanties appropriées / supplémentaires
- Durée de conservation : maximum = durée de conservation fichier central

- Les règles d'accès et de traitement seront arrêtées par la Police sur la base des critères suivants :
  - Détail des informations : s'agit-il d'informations principales / métadonnées ou d'un accès à des documents déterminés, tels que des PV et de rapports ?
  - Motifs (qui dépendent du type de mission policière)
  - Type de traitement (accès, modification, …)
  - Appartenance à un service déterminé
  - Règles spécifiques pour la protection des mineurs
  - Etat de la validation de l'information (données douces réglées spécifiquement dans le cadre du fichier central)

➡ Sanctions pénales pour violation frauduleuse des règles: articles 509-1 à 509-7 du Code pénal

1 Les dispositions applicables à tous les fichiers

2 Les dispositions applicables au fichier central

❑ Finalités

- Vérification des antécédents; aide aux contrôles effectués
- Politique de sécurité intérieure; statistiques
- Analyses criminelles opérationnelles
- Exclusion: données en rapport avec les AT réglés

❑ Catégories de personnes :

- Police administrative et autres missions légales : personnes directement concernées par les mesures / rapports
- Police judiciaire :
  - ❖ Personnes suspectes, condamnées, recherchées, …
  - ❖ Victimes / témoins : pas de consultation pour motif non-judiciaire
  - ❖ Catégories de personnes “données douces” (informants, indices sérieux de participation potentielle à une infraction, …) : pas de consultation pour motif non-judiciare + règles spécifiques d’inscription

Catégories de données :

- Partie “informations principales” (y compris un résumé de l’affaire et les actions policères à prendre sur le terrain) : énumération exhaustive dans la loi
- Partie “documents” (procès-verbaux / rapports) : pas d’énumération précise possible

Relation avec autres fichiers :

- Introduction de données dans le fichier central, si enquête terminée ou autorisation autorités judiciaires
- Pour le reste, L. 1.8.2018 règle l’utilisation des données à d’autres finalités

Durées de conservation et d'archivage :

Option A (sans aucun archivage*) :

- Police judiciaire :
  - Délai de conservation provisoire : crimes / délits : 10 ans – contraventions : 3 ans
  - Par la suite verification état de la procédure auprès des autorités judiciaires : prolongement ou pas
  - Acquittement / rehabilitation après condamnation / prescription action publique: suppression des données
  - Les autorités judiciaires sont libres d'organiser un archivage de leur côté
- Police administrative et autres missions : max. 10 ans de conservation mais possibilité de prévoir des délais plus courts pour des rapports particuliers

Option B (avec un archivage*) :

- Police judiciaire : cf. Option A, toutefois les délais ne donnent pas lieu à une suppression mais à un archivage
- Police administrative et autres missions : max. 10 ans de conservation mais possibilité de prévoir des délais plus courts pour des rapports particuliers
- Archivage :
  - Police judiciaire: archivage 30 ans
  - Police administrative et autres missions : pas d'archivage
  - Accès pour des fins judiciaires avec l'accord du Procureur général d'Etat

* Archivage = une partie passive avec des accès très limités; il ne s'agit pas d'un archive à part

Questions? At your disposal!

Vincent Wellens
Partner, IP, Technology Law & Data Protection
T. + 352 26 12 29 34
E. Vincent.Wellens@nautadutilh.com

Carmen Schellekens
Senior Associate, IP, Technology Law & Data Protection
T. +352 26 12 29 74 06
E. Carmen.Schellekens@nautadutilh.com

Lindsay Korytko
Senior Associate, IP, Technology Law & Data Protection
T. + 352 26 12 29 74 22
E. Lindsay.Korytko@nautadutilh.com

Sigrid Heirbrant
Associate, IP, Technology Law & Data Protection
T. +352 26 12 29 74 50
E. Sigrid.Heirbrant@nautadutilh.com

Emmanuel Thiomé
Associate, IP, Technology Law & Data Protection
T. + 352 26 12 29 74 15
E. Emmanuel.Thiome@nautadutilh.com

Antoine Pétronin
Associate, IP, Technology Law & Data Protection
T. + 352 26 12 29 87
E. Antoine.Petronin@nautadutilh.com