



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Session ordinaire 2019-2020

MW/PR

P.V. SID 10
P.V. J 21

Commission de la Sécurité intérieure et de la Défense

Commission de la Justice

Procès-verbal de la réunion du 5 mars 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. Uniquement pour les membres de la Commission de la Sécurité intérieure et de la Défense :

Approbation des projets de procès-verbal des réunions du 3 octobre 2019 et des 7 et 9 janvier 2020

*

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. Claude Lamberty, M. Georges Mischo, membres de la Commission de la Sécurité intérieure et de la Défense

Mme Diane Adehm, M. François Benoy, M. Dan Biancalana, M. Frank Colabianchi (en rempl. de M. Guy Arendt), Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, Mme Carole Hartmann, Mme Cécile Hemmen, M. Pim Knaff, M. Charles Margue, Mme Octavie Modert, M. Laurent Mosar, M. Gilles Roth, membres de la Commission de la Justice

M. François Bausch, Ministre de 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), M. Alain Braun, Senior Software Developer Team Leader

Inspection générale de la Police (IGP) :

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

M. Gil Goebbels, du Ministère de la Justice

M. Vincent Wellens, NautaDutilh

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : M. Gusty Graas, M. Fernand Kartheiser, membres de la Commission de la Sécurité intérieure et de la Défense

M. Marc Baum, observateur délégué

M. Roy Reding, membre de la Commission de la Justice

M. Marc Baum, observateur délégué

*

Présidence : Mme Stéphanie Empain, Présidente de la Commission de la Sécurité intérieure et de la Défense

*

Avant de passer à l'ordre du jour proprement dit de la réunion, Madame la Présidente donne la parole aux membres du groupe parlementaire CSV qui souhaiteraient exprimer une critique générale.

Tout en saluant les efforts réalisés par les différents acteurs, M. Laurent Mosar (CSV) constate cependant que ce qui a été retenu jusqu'à présent au cours des réunions avec les députés n'est pas encore mis en œuvre au niveau des fichiers, notamment en ce qui concerne la radiation de données. Ceci est particulièrement fâcheux en cas d'acquittement et de non-lieu. L'orateur illustre ses propos à l'aide d'une affaire lui relatée, qui continue à figurer au journal des affaires (JDA) du Service de Police judiciaire malgré un acquittement, et ceci depuis huit mois à partir de la demande de radiation. L'orateur insiste dès lors sur une mise en œuvre rapide des décisions prises, aussi dans l'intérêt de la crédibilité des autorités concernées.

Monsieur le Ministre se déclare par principe d'accord avec cette demande, un tableau qui sera distribué informant sur l'avancement des travaux. Le but poursuivi est d'inclure le maximum dans le fichier central et de régler l'accès de manière stricte en fonction des catégories de données. Le nombre de fichiers particuliers est limité le plus possible. Le tableau mentionné inclut les recommandations de l'IGP¹ et de la CNPD² et sera constamment mis à jour pour pouvoir informer régulièrement les députés sur l'état actuel des travaux. Le comité de suivi, entretemps élargi, se réunit mensuellement et effectue le suivi toujours sur base des recommandations de l'IGP et de la CNPD.

¹ Inspection générale de la Police

² Commission nationale pour la protection des données

Concernant l'exemple donné ci-dessus, un représentant de la Police précise que l'information se trouve dans le fichier central. La Police demande à ce que les mêmes règles s'appliquent à toutes les bases de données, dans le sens que les durées de conservation des données dans un fichier particulier ne seront en aucun cas supérieures à celles qui sont applicables au fichier central, sauf si une disposition légale spécifique prévoit une durée plus longue. Il n'est pas possible de donner immédiatement satisfaction à toutes les demandes de radiation de la partie active du fichier central, alors que la Police doit vérifier que les informations reçues par la personne concernée sont correctes. Il n'est par ailleurs pas possible de rayer les informations automatiquement de tous les fichiers. Des recherches manuelles sont nécessaires afin d'identifier les autres fichiers qui contiennent des données. Il faut malheureusement attendre la mise en place du nouveau système avec un retour systématique de données de la part des autorités judiciaires au niveau du fichier central et une mise à jour des autres outils informatiques afin de disposer d'une possibilité de tenir compte des décisions de justice de façon proactive. Le problème se pose donc de la même manière pour le fichier central que pour les autres fichiers.

Un autre membre de la Police donne un aperçu des travaux actuels. En étroite coopération avec la Justice, la mise en place d'un « nouveau » fichier central est en cours. Si un échange d'informations existe depuis des années de la Police vers la Justice, un retour d'informations ne fait que commencer. Les modalités techniques de mise en œuvre de ce retour sont discutées régulièrement avec la Justice au cours d'entrevues mensuelles ayant pour objet de résoudre les problèmes techniques qui se présentent.

Au cours des deux derniers mois, la Police a envoyé 12 000 affaires à la Justice (depuis le mois de septembre dernier même 70 000) et a été informée jusqu'ici par voie électronique par la Justice de l'évolution déjà d'un quart de ces affaires. Aussi la Justice a-t-elle transmis 17 acquittements. À noter que les chiffres ne sont pas à considérer comme absolus en raison des travaux en cours, l'automatisme ne fonctionnant pas encore.

L'échange d'informations a débuté des deux côtés avec des bases de données, en partie, de 10, voire 20 ans. Les bases respectives, les environnements techniques de part et d'autre, ne correspondant pas, des efforts sont toujours en train d'être faits pour mettre en place les concepts nécessaires sur les vieux systèmes de bases de données. Les travaux ne se limitent donc pas à la mise en place du nouveau fichier central ; la Justice doit également apporter sa contribution et les systèmes de bases de données, comme le JDA, doivent être adaptés. Exprimé en termes techniques, cela signifie apprendre aux vieux systèmes du nouveau. Concrètement, au début de la digitalisation du fichier central en l'an 2000, le support d'enregistrement des données ne permettait aucune modification par la suite. Ce support apportait la garantie technique que les données ne pouvaient être ni modifiées ni supprimées. Le support a été remplacé quelques années plus tard pour permettre la radiation.

Il s'agit donc de faire en sorte que les deux environnements techniques puissent communiquer. Le retour d'informations doit être fiable et automatique. Il est illusoire de penser que le traitement manuel d'aujourd'hui soit suffisant ; si la radiation est devenue possible, il faut néanmoins y procéder de manière manuelle.

Le problème soulevé par M. Mosar tient donc aujourd'hui à un travail purement manuel.

La Police ne peut pas procéder à la radiation à la simple demande d'un citoyen, mais doit avoir une preuve. Pour l'obtenir, elle peut s'informer auprès des autorités judiciaires, sachant pourtant que ceci signifie un volume de travail considérable pour la Police. Si la protection des données est considérée comme objectif suprême, il existe une possibilité : l'autorité compétente donne à la Police l'instruction de procéder à la radiation de toutes les données, dont l'enregistrement n'est pas conforme aux règles actuelles de protection des données, ce qui est le cas pour la majeure partie des données. La réalité est effectivement telle que la

Police ne peut résoudre en quelques semaines les problèmes qui se sont accumulés au cours de nombreuses années.

À son tour, M. Gilles Roth (CSV) s'indigne des délais très longs de traitement des demandes des citoyens, citant un exemple où un citoyen a demandé en été 2019 le relevé des données le concernant qu'il a obtenu finalement le 17 janvier 2020. Les données enregistrées ne se rapportent d'ailleurs non seulement à des avertissements taxés (AT) payés, mais aussi à des faits dénoncés par le citoyen à la Police. La conservation de telles données au-delà du délai nécessaire pour le traitement de l'affaire ne se justifie pas si ce n'est dans un État policier, mais non pas dans un État de droit.

En outre, l'orateur constate un manque de respect à l'égard du législateur du fait que les décisions prises ne sont toujours pas mises en œuvre.

Monsieur le Ministre confirme qu'il maintient sa position que les données concernant les AT payés, donc pour lesquels il n'y aura pas de poursuite judiciaire, sont à radier.

Un représentant de la Police rappelle qu'il a été décidé de ne plus enregistrer les contraventions au fichier central. La Police ne voit en outre aucun problème à la radiation des données relatives aux avertissements taxés payés. Le fichier des AT ne distingue cependant pas entre les différents AT, de sorte qu'en cas de radiation, la preuve d'un délit de grande vitesse ne pourra plus être rapportée. Afin d'éviter ceci, le fichier AT doit d'abord être réorganisé, ces travaux n'ayant cependant pas encore pu être entamés. Comme il a été dit, les problèmes qui se sont accumulés pendant de nombreuses années ne sauraient être résolus endéans deux semaines, l'orateur comprenant néanmoins les critiques exprimées. Un autre exemple est l'ELS (Einsatzleitsystem), où sont enregistrées les données et informations obtenues des citoyens et les démarches policières dans ces affaires. En cas de radiation, les informations obtenues ne pourraient plus être gérées. Par ailleurs, l'IGP se renseigne très souvent auprès de la Police, en cas de plainte d'un citoyen, sur ce qui se trouve à ce sujet dans l'ELS.

Il convient aussi de mentionner le fichier IP (informations policières). En cas de dépôt d'une plainte, un procès-verbal est rédigé et les données sont gérées dans ce fichier. Cet outil est nécessaire pour le retour d'informations par le Parquet. Si une affaire s'étend sur cinq ans jusqu'à la décision définitive, les données doivent pouvoir être conservées pendant la même durée.

Si les critiques ponctuelles sont compréhensibles, il faut être conscient que le problème consiste dans le fait que tous les domaines sont reliés les uns aux autres.

En réponse à une question de Mme Stéphanie Empain (déi gréng), le représentant de la Police explique que les « nouveaux » AT payés sont actuellement également gérés avec le même outil. Le délai général de conservation est de 24 mois pour les AT et de 4 ans pour les contraventions graves en raison du délit de grande vitesse. La radiation immédiate suite au paiement exige une grande prudence afin d'éviter les erreurs en radiant les données d'autrui.

De la part du Ministère de la Sécurité intérieure, il est rappelé que le fichier AT se base sur un règlement grand-ducal du 21 décembre 2004³, lequel prévoit que les données relatives aux avertissements taxés doivent être anonymisées après 24 mois. Dans ce contexte, Monsieur le Ministre a aussi envoyé une lettre à la Police, laquelle a élaboré une solution avec le CTIE⁴ pour la mise en œuvre de cette disposition.

³ Règlement grand-ducal du 21 décembre 2004 portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière et modification du règlement grand-ducal du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales

⁴ Centre des technologies de l'information de l'État

[Extrait du règlement du 21 décembre 2004 précité :

Art. 4. Durée de conservation.

Les données constituant le fichier visé par le présent règlement peuvent être conservées jusqu'à 24 mois après le paiement de l'avertissement taxé, ou en cas de refus de paiement ou de non-paiement endéans les délais légaux de 45 jours, après l'établissement et l'envoi du procès-verbal au Procureur d'Etat territorialement compétent. Au-delà de cette période de 24 mois, les données en question peuvent uniquement être conservées sous forme dépersonnalisée.]

Des difficultés techniques ne représentant pas d'argument pour ne pas donner suite à la décision prise, MM. Mosar et Roth ne se contentent pas d'une déclaration ministérielle faite, même avec détermination, devant les députés et dans les médias, mais revendiquent que Monsieur le Ministre donne, encore avant la prochaine séance publique de la Chambre des Députés, l'ordre par écrit à la Police de procéder à la radiation demandée. En effet, chaque député a le droit dans un État de droit de formuler une telle demande.

Monsieur le Ministre assure que cet ordre sera donné ce jour même et une copie sera transmise aux députés.

Madame le Ministre de la Justice informe les députés sur l'avancement des travaux dans le domaine de la Justice. Concernant l'honorabilité, l'analyse des différents textes est en cours en vue des adaptations nécessaires; une première proposition pour la loi modifiée du 15 mars 1983 sur les armes et munitions est élaborée. L'avis de l'Autorité de contrôle judiciaire est en attente et sera présenté le moment venu aux députés, en incluant dans la mesure du possible les explications sur l'avis de la CNPD, lequel est non encore définitif et confidentiel en raison de la saisine par une personne privée.

*

Au sujet de l'élaboration d'une base légale spécifique pour les traitements de données à caractère personnel effectués par la Police grand-ducale, M. Vincent Wellens informe les députés que le suivi des recommandations de la CNPD et de l'IGP avance. La Police a pu améliorer certains points par quick fixes, d'autres nécessitant plus de temps.

Le but est d'élaborer un cadre légal général pour tous les fichiers et des dispositions spécifiques pour certains fichiers. Un premier avant-projet de loi est actuellement discuté avec les différents acteurs.

Une autre étape qui est également en cours est celle de l'analyse du fonctionnement et du contenu des différents fichiers, la démarche ayant été faite par la Police dans le contexte de la mise en conformité de ses fichiers avec la législation relative à la protection des données. L'IGP a apporté une contribution importante par ses clarifications au niveau de l'identification des types de fichiers. Comme il a déjà été souligné au cours de la réunion du 20 décembre 2019, l'élaboration des dispositions légales pour le fichier central et les autres fichiers doit se faire à la lumière de la réalité du travail policier sur le terrain. Après l'analyse de tous les fichiers, il sera examiné dans quelle mesure des synergies pourront être établies entre ces fichiers (« rationalisation des fichiers (fin 2020) », annexe p. 2). Les travaux comprennent toujours un exercice de bases communicantes, le fichier central étant susceptible de communiquer avec d'autres fichiers. Le plus de temps nécessaire répond à l'exigence d'aller au fond et de livrer du bon travail.

À côté de l'analyse du fonctionnement et du contenu des fichiers, la Police travaille sur la tenue du registre des traitements. Au fur et à mesure de l'avancement des travaux, un feed-in sera fait dans le premier avant-projet de loi.

La réalité a montré que la Police a besoin de plusieurs fichiers; après en avoir identifié la nature, il convient de voir comment on peut les rationaliser avant de se lancer dans la mise en place au niveau informatique. En effet, dans l'intérêt de l'efficacité, il importe de faire d'abord cet exercice de rationalisation au lieu de construire hâtivement une informatique qui ne serait pas en mesure de s'adapter à cette rationalisation des fichiers. En outre, celle-ci correspond aussi aux principes de minimalisation et d'exactitude des données.

De nouvelles dispositions relatives à la protection des données seront insérées dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. Ces dispositions comprendront une partie générale s'appliquant à tous les fichiers de la Police, avec l'indication des différents types. En fonction du type de fichier, on pourra mettre de l'ordre dans les fichiers existants et les rattacher à une catégorie de fichiers (annexe p. 3). Ainsi, dans le système belge, un fichier technique serait celui de la détection automatique des plaques d'immatriculation. Un fichier particulier serait un fichier nécessaire pour la gestion de certaines données, mais sans être intégré au fichier central, notamment pour ne pas surcharger celui-ci avec de telles données.

Concernant les dispositions à insérer dans la loi précitée du 18 juillet 2018, il y a une catégorie optionnelle, celle des fichiers communs, qui est en train d'être discutée. Il peut s'agir de fichiers gérés en commun par la Police et les autorités judiciaires, ou de fichiers pour lesquels la CNPD constate qu'il y a une responsabilité conjointe. Pour ces fichiers, des règles seront proposées pour les encadrer.

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 est transposée par la loi du 1^{er} 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. La CNPD précise dans son avis relatif au fichier central de la Police grand-ducale au regard de la législation sur la protection des données⁵ que cette loi « prévoit de manière générale et encadre l'ingérence qui est faite par les traitements mis en œuvre par les fichiers dans les droits fondamentaux. En effet, cette loi a pour objet de transposer la directive en droit luxembourgeois et *de facto*, de fixer des règles minimales spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes visées à l'article 1^{er} de cette loi. En d'autres termes, même si cette loi n'est pas spécifiquement dédiée à la gestion et à l'exploitation du fichier central, elle encadre néanmoins les traitements dudit fichier utilisé par la Police dans le cadre des missions qui lui sont conférées par la loi [modifiée] du 18 juillet 2018 sur la Police grand-ducale. ».

La directive précitée exige une harmonisation minimale, un socle minimal, les États membres pouvant toujours aller au-delà. La loi précitée du 1^{er} août 2018, la loi de transposition, constitue le cadre légal en la matière. Le but de légiférer dans le domaine des fichiers n'est pas de déroger à cette loi; il s'agit uniquement de préciser des éléments et de le faire par l'insertion de dispositions dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (annexe p. 4).

⁵ CNPD - Délibération n°45/2019 du 13 septembre 2019

Le fichier central fait déjà l'objet de nombre de dispositions dans la loi précitée du 18 juillet 2018. Concernant le dispositif nouveau, certains points seront à régler au niveau du règlement grand-ducal, d'autres au niveau interne de la Police.

Des règles minimales seront établies pour la création, la gestion et l'exploitation des autres fichiers. Pour les fichiers particuliers et techniques, la règle sera le niveau interne pour laisser suffisamment de flexibilité à la Police. La possibilité du règlement grand-ducal sera toujours maintenue, sans revenir au système de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, c'est-à-dire de régler chaque fichier par règlement grand-ducal. En effet, la philosophie de la directive (UE) 2016/680 et 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 données⁶ consiste à responsabiliser les responsables du traitement et à leur permettre de prendre eux-mêmes des décisions.

La loi précitée du 1^{er} août 2018 n'impose pas la voie législative ou réglementaire pour la création d'un nouveau fichier, mais prévoit dans son article 27, paragraphe 1^{er} :

« Art. 27. Consultation préalable de l'autorité de contrôle compétente

(1) Le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle compétente préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer :

- a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 26, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, ou
- b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées. ».

Toutes les autorités visées par la loi précitée du 1^{er} août 2018 peuvent par conséquent déjà créer des fichiers. Concernant les fichiers particuliers, les travaux en cours ont pour objet de mieux encadrer leur création et de voir quels éléments sont à régler au mieux au niveau de la Police. La majeure partie de l'étude était destinée à examiner si les dispositions n'entrent pas par la suite en conflit avec la CNPD, qui veille au respect de la vie privée. Suivant l'article 11, paragraphe 3 de la Constitution: « L'État garantit la protection de la vie privée, sauf les exceptions fixées par la loi. ». Pour la CNPD, la loi doit contenir les éléments essentiels concernant la protection de la vie privée. Il en va de même des délais de conservation qui peuvent être réglés par procédure interne selon l'article 4 de la loi précitée du 1^{er} août 2018; la CNPD considère cette matière comme essentielle et devant être réglée par la loi. Il importe par conséquent de trouver un consensus qui tient la route du point de vue juridique.

Comme l'avant-projet de loi est en train d'être discuté avec les stakeholders, il suffit pour l'instant de se limiter à quelques données générales, pour ce qui est des dispositions communes (annexe p. 6). Tous les fichiers liés aux activités opérationnelles de la Police sont visés; sont donc exclus les fichiers liés aux activités internes, tels les fichiers relatifs aux ressources humaines. Ce régime « par défaut » permet néanmoins au législateur d'adopter par des lois spécifiques des règles différentes, par exemple en matière d'ADN.

Les aspects à régler sont :

⁶ Règlement général sur la protection des données (RGPD), mis en oeuvre par la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre 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

- l'énumération des différentes catégories de fichiers ;
- la spécification du responsable de traitement, à savoir la Police ;
- un meilleur encadrement des données spéciales ;
- la détermination de critères de base pour des règles d'accès, lesquelles seront adoptées au niveau de la Police, et de sanctions pénales pour non-respect intentionnel des règles d'accès, s'il y a une volonté politique pour cela ;
- la détermination de règles pour la communication entre fichiers – certains fichiers doivent communiquer entre eux, cette communication est nécessaire, mais doit être encadrée par des règles précises ;
- la journalisation, déjà prévue par la loi précitée du 1^{er} août 2018, sera complétée par l'inscription dans la loi du principe de motifs circonstanciés de consultation pour chaque fichier créé, ces motifs étant déterminés au niveau de la Police, l'inscription ayant pour but de faire naître une prise de conscience pour la nécessité de tels motifs ;
- la détermination de critères pour la durée de conservation ; vu qu'il existe une multitude de fichiers qui poursuivent différentes finalités, la durée de conservation peut différer selon la finalité. On peut inscrire dans une loi générale les critères à prendre en compte ; concernant le fichier central, il est prévu qu'un règlement grand-ducal détermine les critères. Ceci ne peut être fait pour chaque fichier, mais il importe qu'une règle existe au sein de la Police permettant de savoir quels critères sont à considérer pour la durée de conservation de tel fichier.

Le dernier point important des dispositions communes est celui du régime transitoire à prévoir. La directive (UE) 2016/680 et sa loi de transposition du 1^{er} août 2018 précitées contiennent des règles spécifiques pour la journalisation et prévoient un régime transitoire pour la mise en conformité des bases de données des autorités concernées.

Quant aux règles par catégories de fichiers (annexe pp. 8+9), il y a également des aspects à régler **au niveau de la loi** modifiée du 18 juillet 2018 sur la Police grand-ducale :

- les finalités des fichiers, par exemple pour la refonte du fichier central : coordination et croisement des données et informations policières, vérification des antécédents ; on peut aussi expliquer ce qu'est un fichier technique et comment il fonctionne, mais on ne peut pas englober au niveau de la loi toutes les finalités possibles des fichiers créés sous ce régime ;
- les données : détermination des personnes concernées en veillant à la conformité à la directive 2016/680 : par exemple pour la refonte du fichier central (témoin, victime, suspects, coupables, etc.) ; tenir compte de l'existence ou non d'une partie signalétique (métadonnées) et d'une partie documentaire des fichiers (documents rattachés aux fichiers) ;
- la conservation : détermination de critères plus spécifiques pour les différents types de fichiers ;
- archivage : déterminer un délai d'archivage précis pour les différents types de fichiers ; au niveau de la loi, la détermination d'un délai précis de conservation n'est souvent pas possible ;
- intercommunication des fichiers : détermination de règles spécifiques pour le fichier ou la catégorie de fichier ;
- qualité des données : en ce qui concerne les données « douces » : prévoir comment vérifier la fiabilité de ce type de données ;
- communication et accès aux données : régler l'accès à ces données (y inclus l'accès aux fichiers internes de la Police) et leur communication à d'autres entités, en distinguant entre communication, accès direct (la Police a un accès direct à certaines données) et interrogation directe.

Les aspects à régler plus en détail **au niveau d'une norme inférieure** (règlement grand-ducal et/ou procédure interne de la Police) sont les suivants (annexe p. 10) :

- catégories de données ;
- motifs d'accès, d'interrogation et de communication ;
- délais concrets de conservation des données, en distinguant entre police judiciaire et police administrative ;

- critères et code d'évaluation pour certains fichiers pour apprécier la fiabilité des données, notamment des données « douces ».

M. Laurent Mosar (CSV) exprime ses remerciements et sa satisfaction des explications obtenues et souhaiterait des précisions sur les trois points suivants :

- 1) l'archivage : si le principe de l'archivage des données était maintenu, quelles seraient les données concernées et les règles applicables ? L'orateur rappelle que le CSV plaide plutôt pour l'abandon de l'archivage des données au niveau des fichiers de la Police.
- 2) la suppression et l'annulation de données : il importe que des règles précises soient inscrites dans la loi ;
- 3) l'interconnexion avec les fichiers de la Justice : comment doit-elle fonctionner ?

Ad 1) : M. Wellens explique que si on peut certes en discuter l'étendue et la portée, un archivage devrait rester possible, l'étude comparative des systèmes des pays voisins ayant d'ailleurs révélé que l'archivage constitue toujours une « best practice ». Il convient aussi de préciser que les droits d'accès aux données archivées sont extrêmement limités. Les données archivées sont celles en matière pénale, dont la durée de conservation s'est écoulée.

Monsieur le Ministre indique que des réflexions sont encore en cours à ce sujet, prenant en considération aussi d'autres dispositions légales, telle la loi du 17 août 2018 relative à l'archivage, en ce qui concerne une obligation d'archiver certaines données.

De même, des réflexions sont à faire en ce qui concerne la portée de l'archivage : il doit s'agir de données qui ont une certaine importance, comme l'explique M. Wellens. On ne s'oriente pas sur la loi belge, en vertu de laquelle sont archivées des données devenues non pertinentes.

Ad 2) : La loi du 1^{er} août 2018 précitée pose le cadre par ses dispositions relatives aux droits des personnes concernées (article 15 : « Droit de rectification ou d'effacement des données à caractère personnel et limitation du traitement »). Ces dispositions ne seront pas modifiées, mais pas non plus copiées dans une autre loi.

M. Laurent Mosar insistant sur une précision dans la loi du moment de suppression et des données concernées, Monsieur le Ministre confirme la nécessité d'une catégorisation des données et rappelle le problème technique exposé ci-dessus (cf. pp. 3 et 4), la radiation automatique ne fonctionnant pas encore.

Mme Stéphanie Empain (déi gréng) fait remarquer qu'il s'agit aussi d'une décision politique.

Suite à l'écoulement de la durée de conservation, soit les données sont archivées en raison de leur importance, soit elles ne rentrent pas dans la portée de l'archivage et, dans ce cas, la seule suite logique est leur suppression.

Le groupe parlementaire CSV note avec satisfaction qu'il est envisagé d'inscrire dans la loi des sanctions pénales au lieu de sanctions administratives en cas de violation des dispositions de la loi (cf. ci-dessus p. 8 – aspects à régler). M. Gilles Roth tient toutefois à rendre attentif au deuxième avis complémentaire du Conseil d'État du 28 janvier 2020 relatif au projet de loi 6961 portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 2) du Code pénal, où le Conseil d'État exprime une opposition formelle à l'encontre de la durée de conservation de dix ans des données à caractère personnel figurant dans les fiches succinctes établies en relation avec les habilitations de sécurité des niveaux « CONFIDENTIEL » et « SECRET ». Extrait de l'avis précité du Conseil d'État :

« Amendement 20

Par l'effet de l'amendement sous examen, les auteurs entendent modifier l'article 29 de la loi précitée du 15 juin 2004, pour fixer la durée de conservation des données relatives à l'enquête de sécurité. Les durées retenues à l'alinéa 1^{er} correspondent à celles inscrites actuellement à l'article 23, alinéa 4, de la loi précitée du 15 juin 2004 et n'appellent pas d'observation de la part du Conseil d'État.

Pour ce qui est de la durée de conservation de la fiche succincte inscrite à l'alinéa 2, les auteurs proposent de la prolonger de cinq à dix ans, en expliquant que cette modification « doit permettre à l'autorité nationale de sécurité d'avoir accès, le cas échéant, à certaines informations pertinentes concernant une personne demandant une habilitation de sécurité du niveau « TRÈS SECRET », ceci notamment pour pouvoir disposer des informations relatives à un retrait ou un refus antérieur d'une habilitation de sécurité dont il devra être tenu compte dans l'analyse d'une nouvelle demande d'obtention d'une habilitation de sécurité ». Le Conseil d'État note toutefois que la durée de conservation de dix ans de la fiche succincte n'est pas limitée aux habilitations de sécurité du niveau « TRÈS SECRET », mais qu'elle s'applique aux demandes de tous les niveaux. Alors que le Conseil d'État peut à la limite comprendre le bien-fondé d'une durée de conservation de la fiche succincte de dix ans pour le niveau de sécurité précité, il n'en va pas de même pour les autres niveaux de sécurité. Au regard du principe suivant lequel les données à caractère personnel ne peuvent pas être conservées pendant une durée excédant celle nécessaire aux finalités pour lesquelles elles sont traitées, tel qu'il ressort des règles adoptées par l'Union européenne ainsi que de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée par le Conseil de l'Europe à Strasbourg le 28 janvier 1981⁷, le Conseil d'État doit s'opposer formellement à la disposition sous avis, étant donné que la durée de conservation de dix ans des données à caractère personnel figurant dans les fiches succinctes établies en relation avec les habilitations de sécurité des niveaux « CONFIDENTIEL » et « SECRET » est disproportionnée. »

Dans ce contexte, l'archivage est difficilement concevable pour l'orateur dans le présent domaine.

Ensuite, la protection des données relève du domaine de la vie privée et constitue donc une matière réservée à la loi. Les principes essentiels doivent par conséquent se trouver dans la loi, y compris la journalisation, le droit à l'effacement, de même que les principes fondamentaux concernant la protection des données, dont la durée de conservation. Le CSV demande une loi qui reprenne l'entière du traitement des données à caractère personnel effectués par la Police et qui le règle concrètement, évitant ainsi d'être obligé à faire des recherches dans plusieurs textes pour connaître la législation.

Enfin, l'orateur souhaiterait connaître la suite du dossier et l'échéancier et exprime le désir de voir soumettre un avant-projet de texte aux députés pour pouvoir discuter concrètement.

Monsieur le Ministre assure que la prochaine étape sera la soumission d'un texte, les pré-travaux de finalisation étant à un stade avancé. Au cours des prochaines semaines, certaines questions seront encore élucidées. Une première mouture du texte pourrait être discutée au cours d'une réunion vers la fin du mois de mai ; l'avant-projet, tenant compte des suggestions parlementaires alors faites, pourra ensuite passer au Conseil de gouvernement au mois de juin. Monsieur le Ministre rappelle qu'il est lui-même demandeur pour inscrire dans la loi le maximum de principes généraux, notamment en ce qui concerne les délais.

⁷ Article 5 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981 et ratifiée par le Grand-Duché de Luxembourg le 10 février 1988 (Loi du 19 novembre 1987 portant a) approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg, le 28 janvier 1981 ; b) modification de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, publiée au Mémorial A94 du 27 novembre 1987).

M. Wellens souligne qu'il faut procéder par étapes ; il importe d'obtenir d'abord l'accord des acteurs concernés sur la structure du texte. La complexité de la matière fait qu'on est passé d'un texte « fichier central » à un texte qui couvre également les autres bases de données, ce qui a prolongé la durée des travaux. L'orateur rappelle qu'il existe déjà une base légale, en vertu de laquelle la Police a l'obligation de régler la durée de conservation par procédure interne.

Au sujet de la transparence de la législation à l'égard du citoyen, ce dernier ne voit rien en fait, puisque la Police peut valablement créer de manière interne des fichiers sur base de la loi. Il est prévu d'insérer dans le futur texte certaines mesures de transparence : par exemple, il sera examiné s'il est envisageable de publier certaines prescriptions internes de la Police au Journal officiel. En outre, par analogie à la CNIL⁸ en France, la CNPD approuve l'idée des auteurs du texte de publier une fiche technique reprenant les éléments-clé des fichiers principaux de la Police.

2. Approbation de projets de procès-verbal

Les projets de procès-verbal sont approuvés.

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

⁸ Commission nationale de l'informatique et des libertés

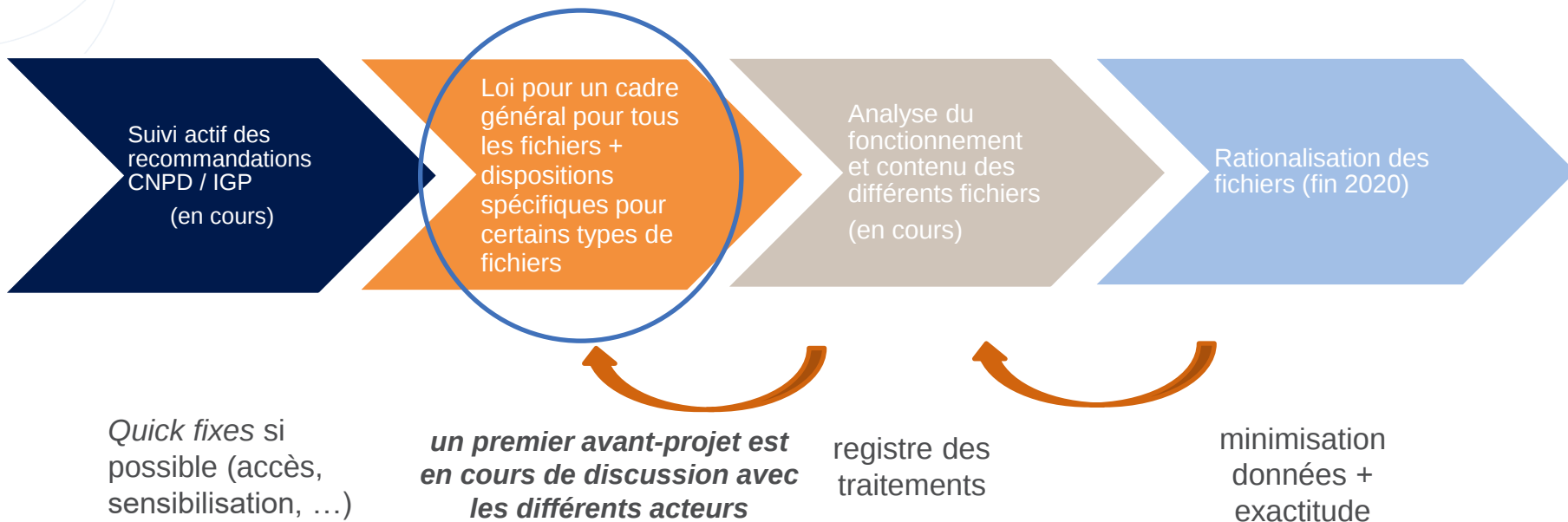


295
years
Est. 1724

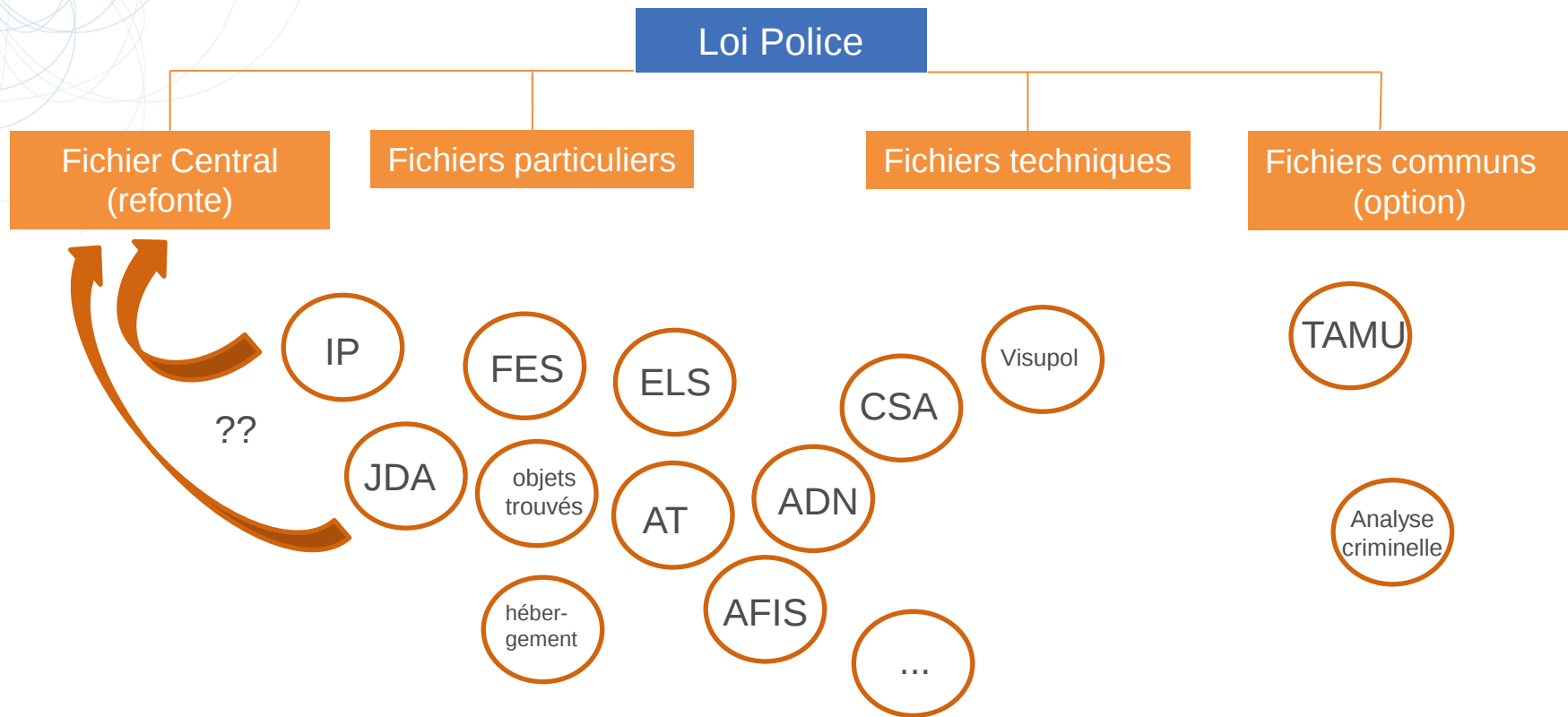
Proposition des grands principes de l'avant-projet de loi sur les fichiers de la Police

5 mars 2020 – Chambre des députés : commission de la Sécurité intérieure et de la Défense

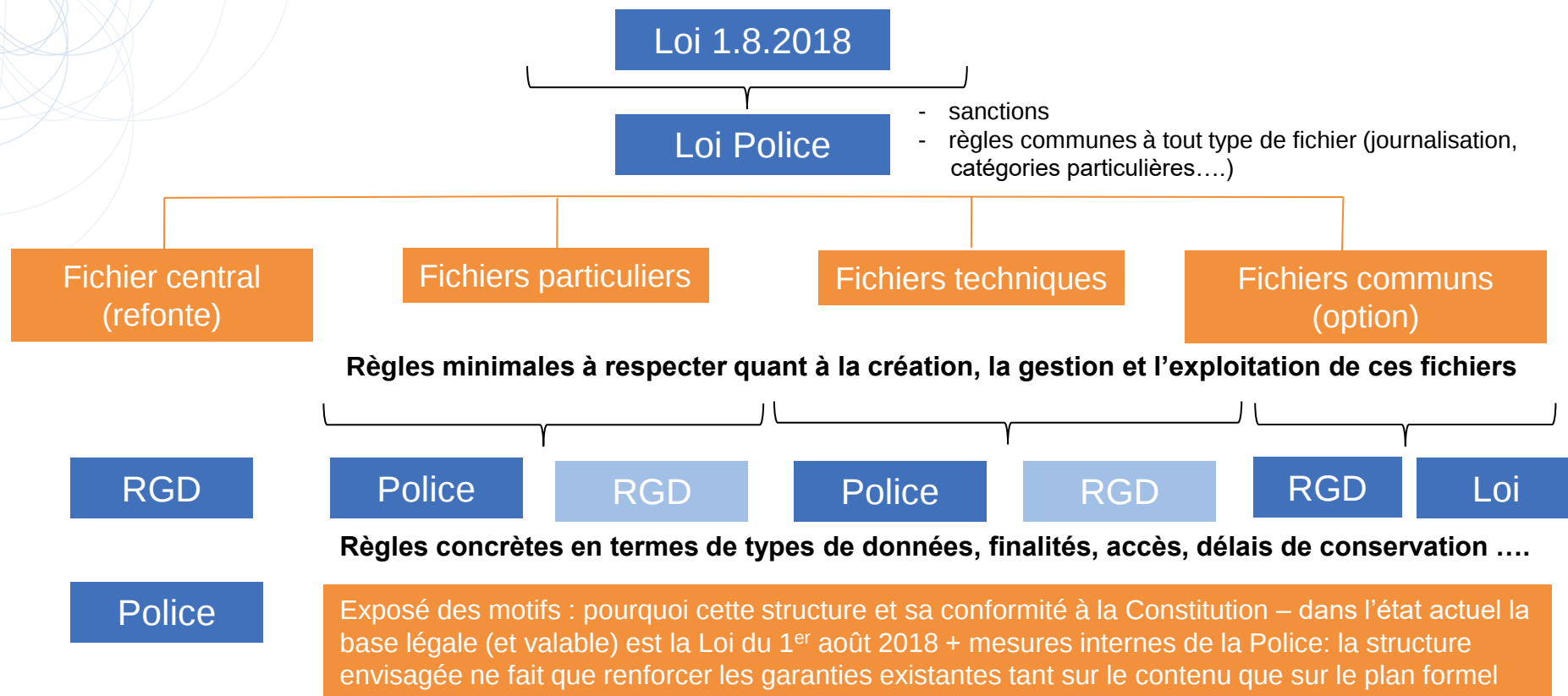
Plan de mise en œuvre



Proposition de structure du nouvel encadrement



Proposition de structure du nouvel encadrement





1

Proposition de règles pour tous les fichiers

2

Proposition de règles pour des (catégories de) fichiers plus spécifiques

Dispositions communes

- ❑ **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)
- ❑ **Aspects à régler :**
 - ❑ énumération des différentes catégories de fichiers,
 - ❑ Police : responsable de traitement
 - ❑ données spéciales (données de santé, données relatives à la conviction politique, religion etc)
 - ❑ critères de base pour des règles d'accès + sanctions pénales pour non-respect intentionnel des règles d'accès
 - ❑ règles sur la communication entre fichiers
 - ❑ critères pour la durée de conservation
 - ❑ journalisation (principe de motifs circonstanciés de consultation)
- ❑ **Dispositions transitoires :** il faudra prévoir un régime de transition



1

Proposition de règles pour tous les fichiers

2

Proposition de règles pour des (catégories de) fichiers plus spécifiques

Aspects à régler au niveau de la loi sur la police

❑ finalités

- ❑ par exemple, pour la refonte du nouveau fichier central: la coordination et le croisement des données et informations policières; vérification des antécédents; aide aux contrôles effectués

❑ données :

- ❑ personnes concernées (par exemple, pour la refonte du nouveau fichier central : avec une distinction entre témoin, victime, suspects, coupables, ...)
- ❑ l'existence ou non d'une partie signalétique / documentaire
- ❑ données "douces"

❑ conservation : critères (guidés par la nécessité de la conservation)

❑ archivage : délai concret

Aspects à régler au niveau de la loi sur la police

- ❑ **communication avec autres fichiers:** règles spécifiques pour le fichier ou la catégorie de fichier en question
- ❑ **qualité des données:** principe de l'exactitude de données
- ❑ **communication et accès aux données :** avec une distinction entre communication / accès direct / interrogation directe

Aspects à régler au niveau d'une norme inférieure (RGD et/ou procédure de la Police)

- ❑ **catégories de données:** partie signalétique (avec categories de données) et partie documentaire
- ❑ **motifs d'accès / interrogation / communication**
- ❑ **délais concrets de conservation police judiciaire / administrative**
- ❑ **critères et code d'évaluation pour certains fichiers / données (données douces)**



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