Session ordinaire 2019-2020

MW/PR

P.V. SID 05
P.V. J 13

Commission de la Sécurité intérieure et de la Défense

Commission de la Justice

Procès-verbal de la réunion du 20 décembre 2019

Ordre du jour :

1. Présentation des premières pistes pour l'élaboration d'une base légale spécifique pour les traitements de données à caractère personnel effectués par la Police grand-ducale

2. Informations sur la mise en oeuvre 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

*

Présents : Mme Diane Adehm, Mme Semiray Ahmedova, Mme Nancy Arendt épouse Kemp, M. Carlo Back, M. André Bauler, Mme Simone Beissel (en rempl. de M. Max Hahn), M. Mars Di Bartolomeo (en rempl. de M. Dan Biancalana), Mme Stéphanie Empain, M. Georges Engel, M. Marc Goergen, M. Gusty Graas, M. Aly Kaes (en rempl. de M. Léon Gloden), M. Fernand Kartheiser, membres de la Commission de la Sécurité intérieure et de la Défense

Mme Diane Adehm, M. Guy Arendt, M. Alex Bodry, M. Mars Di Bartolomeo (en rempl. de M. Dan Biancalana), Mme Stéphanie Empain, M. Marc Goergen, Mme Carole Hartmann, M. Aly Kaes (en rempl. de M. Léon Gloden), M. Charles Margue, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, 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, du Ministère de la Sécurité intérieure

Police grand-ducale :

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

M. Luc Reding, M. Gil Goebbels, du Ministère de la Justice

M. Vincent Wellens, Nauta*Dutilh*

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : M. Jean-Marie Halsdorf, M. Georges Mischo, membres de la Commission de la Sécurité intérieure et de la Défense

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

*

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

*

1. Présentation des premières pistes pour l'élaboration d'une base légale spécifique pour les traitements de données à caractère personnel effectués par la Police grand-ducale

Après avoir exposé brièvement l'ordre du jour de la réunion, Madame la Présidente passe la parole à Monsieur le Ministre qui précise qu'il ne s'agit pas uniquement de l'élaboration de textes législatifs et réglementaires, mais qu'il importe aussi de réaliser la mise en œuvre technique d'une série de propositions sans passer par la voie législative (« quick fixes »). La présentation à l'ordre du jour est destinée à donner un premier aperçu, tenant compte des différents avis. Le suivi des travaux est assuré par le comité de suivi instauré par le ministère et les députés seront régulièrement informés sur l'état des travaux, Monsieur le Ministre proposant de tenir une prochaine réunion jointe le 5 mars 2020. De nombreux points sont à trancher en commun avant le dépôt d'un texte, Monsieur le Ministre accordant une grande importance à l'avis des députés.

Le cabinet Nauta*Dutilh* a été mandaté de faire une ébauche des premières pistes qui pourraient être suivies pour donner un cadre légal au fichier central de la Police grand-ducale, de même qu'un cadre général pour les autres bases de données qui se chiffrent à plus de soixante. Le résultat de ces travaux est présenté à l'aide d'un document PowerPoint (cf. annexe).

Le fichier central et les autres fichiers ont déjà une base légale, à savoir 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. Il existe donc déjà un cadre général appliqué par les organes travaillant dans le domaine pénal, parmi lesquels la Police. Encore faut-il lire la loi précitée avec celles relatives au métier policier, à savoir la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, le Code d'instruction criminelle et certaines lois spécifiques.

Une base légale existe par ailleurs pour d'autres éléments, telles les données dites douces (« soft intelligence »), qui ne sont pas rattachés à une infraction en tant que tels et, de ce fait, pourraient être perçus comme illégaux, comme n'ayant pas de base légale. Ces éléments sont à clarifier en raison de cette perception.

Le troisième volet de la problématique concerne les conditions et modalités des traitements effectués par la Police. Se pose avant tout la question de l'accès aux données (« access management ») : qui peut avoir accès à quel type de données ? Une importance accrue revient aussi à la question de la durée de conservation des données. L'article 4 de la loi précitée du 1er août 2018 constitue la base légale :

« **Art. 4. Délais de conservation et d'examen**

(1) Le responsable du traitement fixe des délais appropriés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Les délais sont à fixer eu égard à la finalité du traitement.

(2) Le responsable du traitement établit des règles procédurales en vue d'assurer le respect de ces délais qui déterminent les personnes intervenant au nom et pour compte du responsable du traitement dans cette procédure, y compris le délégué à la protection des données, ainsi que les délais dans lesquelles ces personnes doivent accomplir leurs tâches respectives. Les règles procédurales sont mises à la disposition de la personne concernée conformément à l'article 11 et à l'autorité de contrôle compétente sur demande de celle-ci. ».

Il convient de souligner que la Police a commencé à travailler sur la problématique bien avant la médiatisation de l'affaire dite du « casier *bis* ». En outre, la Commission nationale pour la protection des données (CNPD) ayant entretemps rendu, sur demande du ministre, un avis sur le fichier central et l'Inspection générale de la Police (IGP) ayant réalisé une étude sur les fichiers de la Police, celle-ci est en train de régler déjà des « quick fixes », notamment en ce qui concerne l'« access management » et la sensibilisation des membres de la Police.

Dans le contexte de l'élaboration des textes de loi pour le fichier central et les autres fichiers, à la lumière de la réalité du travail policier sur le terrain, une analyse du fonctionnement et du contenu de tous les fichiers est en cours. Après la vérification de tous les fichiers, il sera examiné dans quelle mesure des synergies pourront être établies entre ces fichiers (« rationalisation des fichiers + réconciliation avec fichiers d'interconnexion (fin 2020) », p. 3, annexe).

Une mini-étude comparative avec la Police d'autres pays a montré d'importantes divergences concernant l'organisation de la Police. Ainsi, en Allemagne, beaucoup de points sont réglés au niveau des Länder, mais pas de manière harmonisée. Au Royaume-Uni, le délai de conservation des données policières est de cent ans. Malgré les différences, un point commun a été trouvé : les autres pays disposent d'un cadre législatif propre au traitement des bases de données policières. Chacun des pays étudiés a aussi un certain traitement des données douces (soft intelligence) ; en Belgique, il n'aurait pas été possible de suivre les traces des terroristes ayant commis les attentats à Bruxelles sans les données douces.

Le benchmarking porte notamment sur la question de savoir s'il faut ou non une loi spécifique. S'agissant des délais de conservation, la question est examinée évidemment à partir de la réalité et de la législation luxembourgeoises, mais le benchmarking peut toujours s'avérer utile, par exemple pour voir si un délai n'est pas excessif.

Les grands principes à réconcilier sont ceux de l'efficacité policière, du respect des engagements internationaux et du respect de la vie privée.

La proposition pour le nouveau cadre législatif se subdivise en deux grands sous-thèmes : d'abord la détermination de la structure du dispositif législatif, ensuite celle des dispositions matérielles.

- Concernant la structure, il faut se référer toujours à la loi-cadre, c'est-à-dire la loi précitée du 1er août 2018, qui couvre tous les aspects du cycle de vie d'une donnée à caractère personnel. Ainsi, la collecte de telles données est implicitement liée à leur traitement subséquent, un traitement n'étant pas possible sans support informatique ou autre, donc sans base de données.

Dans ce contexte, il faut souligner que certaines critiques exprimées dans le passé peuvent parfaitement être solutionnées sur la base de la loi précitée du 1er août 2018. Cette loi prévoit

le principe de minimisation de données : le principe de traiter le minimum possible de données et uniquement si ce traitement est nécessaire à la finalité recherchée. La loi précitée du 1er août 2018 ne fixe pas de délais de conservation des données précis pour les organisations et entreprises privées ; celles-ci doivent veiller à définir une finalité et à ne pas aller au-delà, aussi en ce qui concerne l'accès aux bases de données. La loi du 1er août 2018 prévoit dans quel cas une analyse des risques portant sur la sécurité des données (analyse d'impact sur la protection des données / Data Protection Impact Assessment – DPIA) doit être faite. Elle contient en outre des dispositions spécifiques relatives au droit des personnes concernées.

À la question de la nécessité d'un nouveau dispositif légal, la CNPD a donné une réponse affirmative. Comme mentionné plus haut, les pays qui ont fait l'objet d'une mini-étude disposent d'un cadre législatif propre au traitement des bases de données policières, en particulier sur la base de données centrale. Le niveau de précision varie cependant, surtout pour les bases de données plus spécifiques. D'autres pays n'ont pas de législation spécifique, mais se fondent sur leur loi « nationale » qui équivaut à la loi luxembourgeoise précitée du 1er août 2018.

Il faut se rappeler que la fonction de la Police dans notre société exige une certaine flexibilité dans les travaux législatifs pour assurer son efficacité et sa réactivité. Ainsi, en France, une grande partie de la matière est réglée de manière très précise dans la législation ; néanmoins, une base de données *ad hoc a* été créée en relation avec le mouvement des gilets jaunes. Certains éléments seront donc réglés au niveau de la loi et d'autres à des niveaux inférieurs dans la hiérarchie des normes. (p. 9, annexe)

La proposition de catégorisation des fichiers comprend d'abord le fichier central, subdivisé, conformément à l'étude IGP, en une partie « administrative » et une partie « judiciaire » (cf. Belgique), puisqu'il s'agit de deux fonctions différentes, ce qui a aussi un impact sur les délais de conservation.

Une ouverture sera prévue dans la loi pour adopter des fichiers particuliers, c'est-à-dire des fichiers contenant des données à caractère personnel, dont la centralisation dans le fichier central serait excessive ou non pertinente (p.ex. objets trouvés), ou simplement impossible du point de vue technique (p.ex. empreintes digitales). La loi définit les règles de base pour les fichiers particuliers ; les fichiers concrets seront réglementés, soit par règlement grand-ducal, ce mécanisme ayant déjà été prévu par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, laquelle couvrait aussi le volet pénal, soit au niveau de la Police, la décision étant entourée de mesures de sécurité, dont notamment l'avis de la CNPD.

Une autre catégorie est celle des fichiers techniques, issus d'outils techniques qui enregistrent automatiquement des données de manière structurée (cf. projet en cours pour l'enregistrement automatique des plaques d'immatriculation). Pour ces fichiers également, la loi définit les règles de base et les fichiers concrets sont réglés au niveau législatif, réglementaire ou ministériel sur avis, pour ce dernier, du DPO et, en principe, de la CNPD.

La dernière catégorie est constituée des fichiers communs qui relèvent de la responsabilité conjointe de plusieurs autorités, un exemple en étant le RENITA[1].

S'agissant de la transparence en la matière (p. 14, annexe), un point a été abordé brièvement avec la CNPD, à savoir la mise en place d'une description « high level », sur le site de la CNPD, des principaux types de fichiers qui existent auprès de la Police et de leur mode de fonctionnement.

[1] Réseau National Intégré de Radiocommunication pour les services de sécurité et de secours

○ Quant aux dispositions matérielles, il ne s'agit pas de reprendre le contenu de la loi précitée du 1er août 2018, mais de la compléter en concrétisant les principes.

Parmi les aspects communs aux fichiers se trouve l'identification du responsable du traitement (p. 17, annexe).

Le nouveau dispositif législatif communiquera avec la loi-cadre et spécifiera notamment les cas où l'accès aux données a lieu indirectement à travers la CNPD, le principe se trouvant dans ladite loi-cadre du 1er août 2018 (article 16). En outre, il organisera mieux la transparence, laquelle ne s'exprime pas seulement par le libellé du texte de loi, mais aussi en précisant l'exercice concret du droit à l'information des personnes concernées.

Le principe du « need to know » sera inscrit au nouveau dispositif législatif, en faisant le split entre police judiciaire et police administrative (p. 19, annexe). Seront en outre réglés les détails par type de fichier, l'accès direct, le transfert de données et l'interconnexion entre les fichiers. La journalisation sera réglée de manière plus précise que dans la loi du 1er août 2018, en citant comme exemple la pratique où un agent A contacte un agent B ayant accès au fichier dont l'agent A a besoin. Ce contact n'était pas journalisé jusqu'à présent ; entretemps, la Police l'a réglé par la voie des « quick fixes ».

Un volet d'une importance particulière est le traitement des données sensibles, dont celles concernant les mineurs.

Pour ce qui est des sanctions, autre aspect à régler (p. 21, annexe), les discussions sont en cours. La loi précitée du 1er août 2018 prévoit une sanction pénale à l'égard du membre de la Police en cas de violation de certaines dispositions spécifiques ; en Belgique, est même puni pénalement l'agent de police qui n'alimente pas correctement le fichier central, en n'enregistrant pas toutes les données. Il convient donc de procéder avec prudence dans la rédaction du texte de loi et de trouver un équilibre.

Au niveau du fichier central, les différentes catégories de données seront précisées, en donnant un statut particulier aux informations douces et aux informations concernant les mineurs.

Une distinction sera faite entre les personnes concernées (témoin, victime, suspect, auteur d'une infraction), cette distinction étant applicable aux nouveaux dossiers et, dans la mesure du possible, aux dossiers existants. En plus, un plan de contrôle de la qualité des données sera établi sur base du reflux de données de la part des autorités judiciaires. Ceci amènera à une qualité améliorée des données. (p. 23, annexe)

Le cabinet Nauta*Dutilh* est en train de réfléchir avec le comité de suivi sur les critères de détermination des délais de conservation des données, dont le critère de l'issue d'une affaire, celui des personnes concernées (un témoin ou une victime aura plus qu'un suspect ou un auteur d'une infraction un « right to be forgotten »). Il faut par ailleurs tenir compte de l'expérience de terrain acquise par la Police. Les délais pour les informations douces seront réduits, tandis que dans des cas préalablement définis, un allongement des délais s'impose.

Une distinction doit être faite entre la conservation et l'archivage des données, ce que la loi luxembourgeoise fait déjà. Après l'expiration du délai de conservation, les données sont archivées sous des conditions très strictes, comme tel est le cas déjà aujourd'hui.

Discussion

❖ Au sujet du dispositif législatif proposé, certains éléments étant à régler au niveau de la loi et d'autres à des niveaux inférieurs dans la hiérarchie des normes, M. Laurent Mosar

(CSV), tout en comprenant la motivation, rend attentif à l'exigence du Conseil d'État de régler le maximum dans la loi. Il importe donc de veiller à ne pas trop recourir à l'instrument du règlement grand-ducal.

Monsieur le Ministre explique que la loi précitée du 1er août 2018 est la loi-cadre en matière de traitement des données à caractère personnel en matière pénale. Ensuite, deux lois détermineront les règles de base respectivement pour le fichier central et les fichiers particuliers. Les modalités d'exécution feront l'objet de règlements grand-ducaux et à partir de ceux-ci, certains éléments pourront être déterminés au niveau du ministère ou de la Police, selon la matière.

M. Wellens rappelle qu'il est déjà aujourd'hui possible pour la Police de créer des bases de données liées à son activité, de sorte qu'on se trouve un peu entre deux feux. Il s'agit donc d'encadrer cette possibilité et, pour ajouter une garantie supplémentaire, on adopte une approche ascendante (bottom-up) en réfléchissant à la possibilité de régler certains points critiques par règlement grand-ducal, tout en restant conforme à la ligne du Conseil d'État. Le fichier central actuel s'est basé sur un règlement grand-ducal, renouvelé 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, laquelle prévoyait justement cette ouverture de procéder par voie réglementaire.

Se montrant étonné du maintien d'un archivage de données, alors que la Police a plaidé dans le passé plutôt pour l'abandon de l'archivage, M. Mosar souhaiterait en connaître les motifs.

M. Wellens indique que cette distinction, qui est certes à discuter, est également maintenue dans les pays voisins. Dans des cas critiques, l'archivage peut présenter toute son utilité et il est d'ailleurs encadré de règles strictes. Le fil conducteur en matière de protection de données est toujours la nécessité.

Pour M. Mosar, le principe doit toujours être celui de l'absence d'archivage, donc l'inverse, l'exception étant réservée aux cas critiques. La question de la nécessité d'un archivage demeure pertinente pour le CSV.

L'orateur voudrait également avoir des précisions sur la suppression de données, voire la suppression automatique, notamment en cas d'acquittement et de non-lieu, ce volet ne figurant pas tel quel parmi les propositions présentées.

Les discussions étant encore en cours avec le comité de suivi, il serait prématuré de faire déjà des propositions concrètes. Ce qui est clair, comme l'indique M. Wellens, c'est que les pratiques actuelles seront modifiées ; l'issue d'une affaire judiciaire aura un impact direct sur les modalités de conservation des données.

❖ Pour M. Gilles Roth (CSV), la présentation confirme que la loi précitée du 1er août 2018 détermine déjà tous les principes de base en la matière. S'agissant du principe de la minimisation de données (cf. supra), l'orateur constate toutefois que les fichiers contiennent aujourd'hui de nombreuses données qui ne correspondent pas à ce principe. Il faut tenir compte de la réalité que, dans un grand pays, l'anonymat de l'individu par rapport à l'administration est beaucoup mieux assuré que tel peut être le cas au Luxembourg. Il en va de même pour le droit des personnes concernées, en ce qui concerne la journalisation.

La Police devrait déjà être en mesure aujourd'hui d'appliquer ces principes dans l'attente d'une loi, à l'instar des pays voisins. Le droit au respect de la vie privée est concerné ici ; étant un droit garanti par la Constitution, il s'agit d'une matière réservée à la loi. L'orateur rejoint M. Mosar dans sa demande d'inscrire le maximum dans la loi.

Selon M. Roth, l'accès illicite à des données qui vont au fond de la vie privée d'une personne, parmi lesquelles comptent ses « contacts » avec la Police, étant une matière très sensible (tout comme celle des données médicales qui devrait également faire l'objet d'une révision), devrait à nouveau constituer une infraction, plus précisément : l'accès non autorisé, l'enregistrement incorrect de données, c'est-à-dire selon sa propre appréciation, de même que la communication de données à des tiers, tels les médias. Une amende administrative n'est pas suffisante comme sanction, dès que l'élément intentionnel existe et qu'on n'est donc pas en présence d'une manipulation erronée. Il convient de revenir sur la décision, prise pour la loi précitée du 1er août 2018, de ne plus considérer un tel accès comme infraction.

Monsieur le Ministre partage cette opinion et renvoie à la p. 22 de la présentation.

Quant aux moyens à disposition de la Police, il assure que le système informatique sera entièrement mis à jour ; le budget a été considérablement augmenté et la Police a obtenu l'autorisation ministérielle de recourir à l'aide d'un bureau informatique externe.

Comme l'expose M. Gilles Roth, nonobstant les travaux nécessaires encore à réaliser, le CSV insiste à ce que Monsieur le Ministre et, le cas échéant, également Madame la Ministre de la Justice, donnent l'instruction politique à leurs administrations, dont fait donc partie la Police, d'établir dès à présent les règles concrètes concernant :

1. la limitation des personnes ayant accès aux données ;
2. la détermination des données à conserver ; ainsi, les données en relation avec des avertissements taxés payés ne sont pas à stocker, ce qui peut parfaitement être réglé par une instruction de service ;
3. l'impossibilité d'accès sur base de critères standard, mais seulement à travers l'identification, avec une notification spécifique.

Il s'agit en fait de mettre en œuvre les défaillances décelées par la CNPD et l'IGP.

Monsieur le Ministre se rallie à cette demande et fait savoir que ces discussions sont menées au sein du comité de suivi en vue d'une mise en œuvre rapide. La Police fait d'ailleurs preuve de bonne volonté de mettre en pratique ces mesures.

M. Roth demandant d'informer les députés au cours d'une prochaine réunion sur le suivi de l'instruction à donner aux administrations, Monsieur le Ministre renvoie à sa proposition d'organiser une réunion jointe le 5 mars 2020.

❖ M. Alex Bodry (LSAP) fait remarquer que la proposition opère un retour partiel au système d'avant la loi du 1er 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. Ce qui reste du changement de paradigmes introduit par cette loi et le règlement (UE) 2016/679 précité est le contrôle a posteriori (donc abandon de l'autorisation préalable du système antérieur). On note cependant par rapport au système antérieur qu'il est prévu d'inscrire plus de détails dans les textes de loi et de régler plutôt l'exécution technique dans des règlements grand-ducaux. Il importe alors d'avoir ces règlements à disposition au moment du vote de la loi. L'orateur s'étonne dans ce contexte des exigences qu'aurait le Conseil d'État entretemps, alors qu'il se montrait d'accord avec la loi précitée du 1er août 2018, laquelle laisse au responsable du traitement toute la responsabilité de régler en détail tous les principes inscrits dans cette loi, donc de procéder par voie interne.

M. Bodry souligne l'importance de trouver un équilibre et de faire preuve de flexibilité, afin de permettre à la Police de faire son travail de manière adéquate, donc d'avoir aussi accès aux données nécessaires.

❖ En réponse à une question de M. Marc Goergen (Piraten) de savoir si la Belgique, à laquelle les travaux semblent se référer en particulier, est considérée comme ayant le meilleur système en Europe, M. Wellens explique que tel n'est pas le cas, mais que la Belgique figure parmi d'autres pays ayant fait l'objet du benchmarking pour trouver un équilibre et ne mettre ni tout dans la loi ni laisser trop aux règlements.

M. Goergen estime nécessaire de préciser à la p. 22 de l'annexe les métadonnées enregistrées au fichier central. Il voudrait aussi savoir comment le citoyen pourra consulter les données le concernant, une consultation par voie numérique présentant l'avantage de la simplicité. Cette question est à régler dans la loi elle-même, de même que celle du login, c'est-à-dire d'inscrire dans la loi que les données de login sont conservées pendant la même durée que celle de l'archivage des données consultées.

M. Wellens réaffirme que la loi du 1er août 2018, qui, lue avec la loi précitée du 18 juillet 2018 et le Code d'instruction criminelle, constitue la base légale en la matière, ce que confirme la CNPD, contient déjà des dispositions claires relatives à l'accès du citoyen. Les travaux continueront sur cette base ; il faut voir si l'un ou l'autre fichier est à remodeler et comment cela peut être fait.

Pour ce qui est du login, il s'agit d'un des paradoxes en matière de protection des données : il faut prévoir des mesures de sécurité qui, à leur tour, donnent lieu à la génération d'autres données. L'analyse du système belge de journalisation concernant le fichier central a révélé qu'il y a peu à ajouter au Luxembourg, puisque la loi du 1er août 2018 contient déjà de nombreuses dispositions. La question du délai de conservation des métadonnées est tout à fait intéressent et aussi un peu « circulaire » : qui a accès aux métadonnées ? La demande est notée et ce point sera inclus dans le dispositif législatif.

2. Informations sur la 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

Monsieur le Ministre informe les députés sur l'état actuel des travaux du comité de suivi.

Au niveau de la Police, celle-ci recherche dans la mesure du possible des « quick wins », les possibilités étant cependant pour certains points limitées d'un point de vue technique.

Conformément à une demande formulée par la CNPD et l'IGP, une note a été émise pour rappeler l'importance de la protection des données, en précisant les grands principes avec l'accent sur les données concernant les mineurs. Et surtout sont annoncés les contrôles qui auront désormais lieu, à savoir des contrôles inopinés et des contrôles en cas de violation de la législation applicable en matière de protection des données. Ces contrôles seront effectués par le DPO ou les autorités prévues par les textes de loi.

Monsieur le Directeur général de la Police grand-ducale assure que les membres de la Police ont conscience de l'importance de la protection des données. La sensibilisation étant renforcée au niveau de la formation, il importe que le citoyen puisse se fier à un maniement responsable des données.

Monsieur le Ministre renvoie au Code de déontologie qui consacre une partie à la protection des données.

Sur le plan technique, les travaux avancent en matière de retour d'informations, en particulier du JUCHA[2], et en ce qui concerne la mise en place d'un nouveau fichier central. En effet, les outils informatiques de la Police rendent nécessaires, en raison de leur vétusté, cette mise en place, puisqu'ils ne permettent pas de répondre à toutes les exigences de protection des données.

Au niveau du comité de suivi, surveillant la mise en œuvre des recommandations de l'IGP et de la CNPD, les travaux avancent également bien. La proposition relative aux délais de conservation des données a fait l'objet de discussions approfondies ; celles concernant une autre proposition, relative à l'accès aux bases de données, viennent d'être entamées, en insistant sur la détermination des motifs justifiant l'accès et des personnes ayant accès, soit d'office sur base de leur travail ou fonction, soit pour motif spécial vérifié au cas par cas.

Ensuite, la catégorisation des données enregistrées au fichier central sera détaillée (témoin, victime, auteur…).

Enfin, les recommandations de l'IGP font l'objet d'une analyse détaillée pour voir ce qui peut être réalisé directement dans l'optique des « quick wins » et ce qui nécessite des efforts supplémentaires au niveau de la technique et des ressources humaines.

Monsieur le Ministre estime que des clarifications pourront être données à la réunion prévue au mois de mars au sujet des questions relatives à l'accès aux données, aux délais de conservation et au lien avec le fichier de la Justice.

En réponse à une question de M. Laurent Mosar (CSV), saluant les efforts des acteurs, il est confirmé que les propositions qui seront présentées aux députés auront préalablement trouvé l'accord notamment de l'IGP et de la CNPD, lesquelles sont représentées au comité de suivi.

Rappelant le devoir que remplit la Police et qui nécessite l'accès à des données, M. Carlo Back (déi gréng) souligne que la qualité des données joue un rôle important. Des informations à ce sujet seraient souhaitables au cours de la prochaine réunion.

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

[2] Base de données nationale de la justice pénale (Justice Chaîne Pénale)

Proposition de projet de loi sur le fichier central de la police et un cadre général pour les autres bases de données

20 décembre 2019 – Chambre des députés : commission de la Sécurité intérieure et de la Défense

Les problématiques soulevées récemment

Fichier central

- base légale: L.1.8.2018 jo. Loi Police – Code d'instruction crim. - …

- *soft intelligence*
- structure de la loi

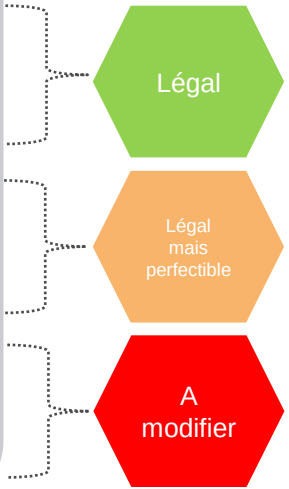
- conditions et modalités des traitements

Prolifération n° fichiers

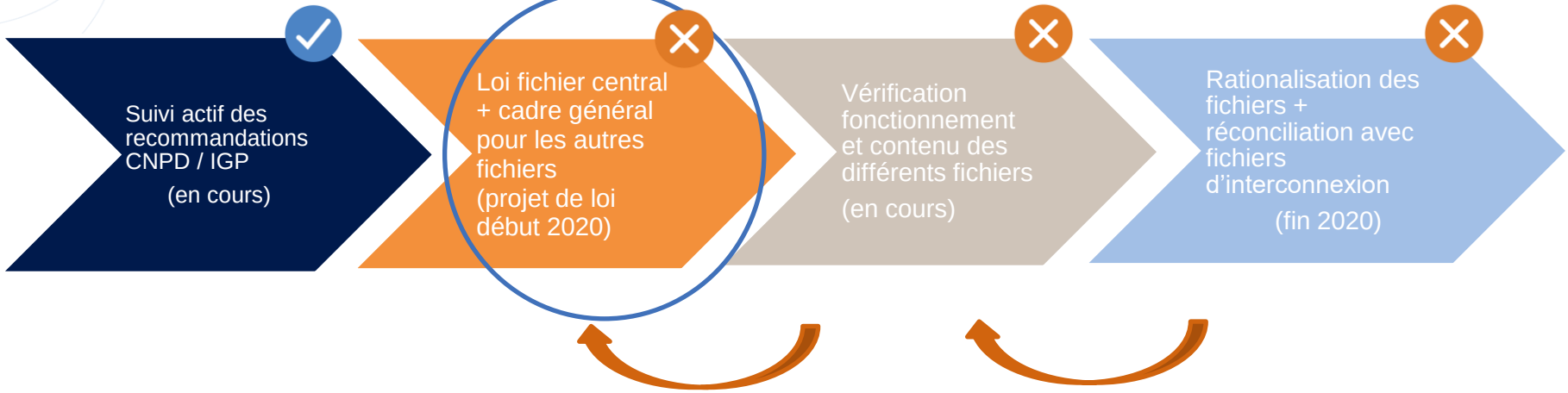
- base légale: L. 1.8.2018 jo. Loi Police – Code d'instruction crim. - …

- redondance entre différents fichiers
- structure de la loi

- structure de la loi
- conditions et modalités des traitements



Plan de régularisation / perfectionnement



Quick fixes si possible (accès, sensibilisation, …)

registre des traitements

minimisation données + exactitude

Etude comparative BE / FR / D / UK / NL

Divergences importantes:

- Dans l'organisation de la police
- Dans la structure du cadre normatif
- Dans le contenu des règles édictées (p. ex. délais de conservation)

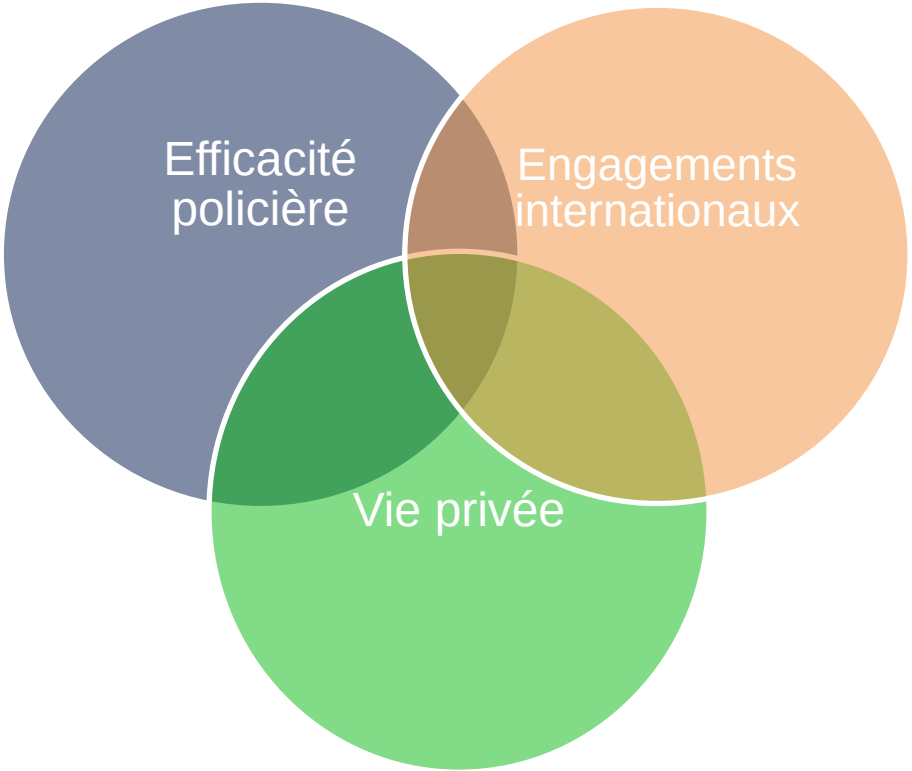
Point commun:
cadre législatif propre traitant des bases de données policières

Point d'attention:
collecte et traitement de *soft intelligence*

Benchmarking

Loi spécifique, délais de conservation …

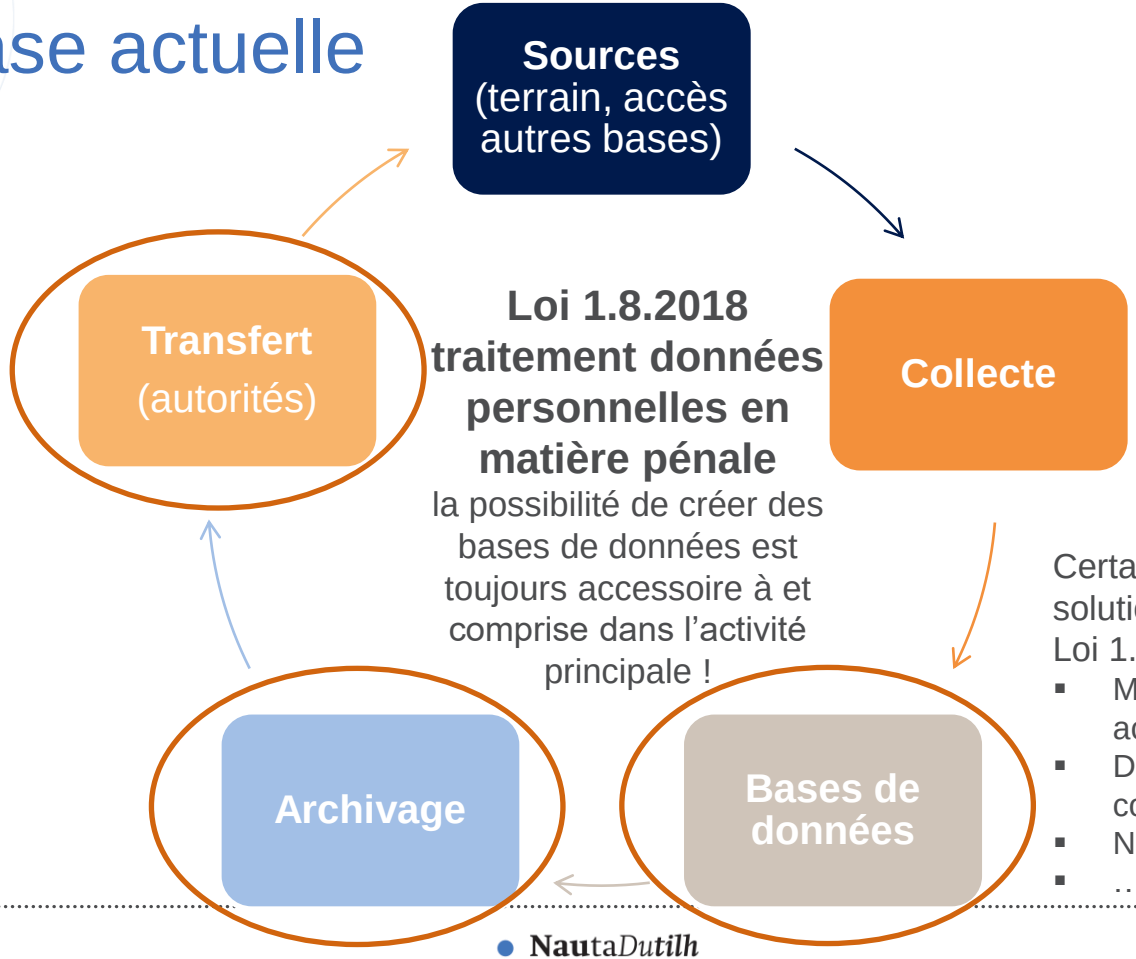
Grands principes à réconcilier



1 Proposition pour la structure du nouveau dispositif législatif

2 Dispositions matérielles

La base actuelle



Certaines critiques peuvent être solutionnées sur la base de la Loi 1.8.2018 :

- Minimisation de données: accès + conservation
- Droit des personnes concernées
- Nécessité DPIA
- …

La nécessité d'un nouveau dispositif légal

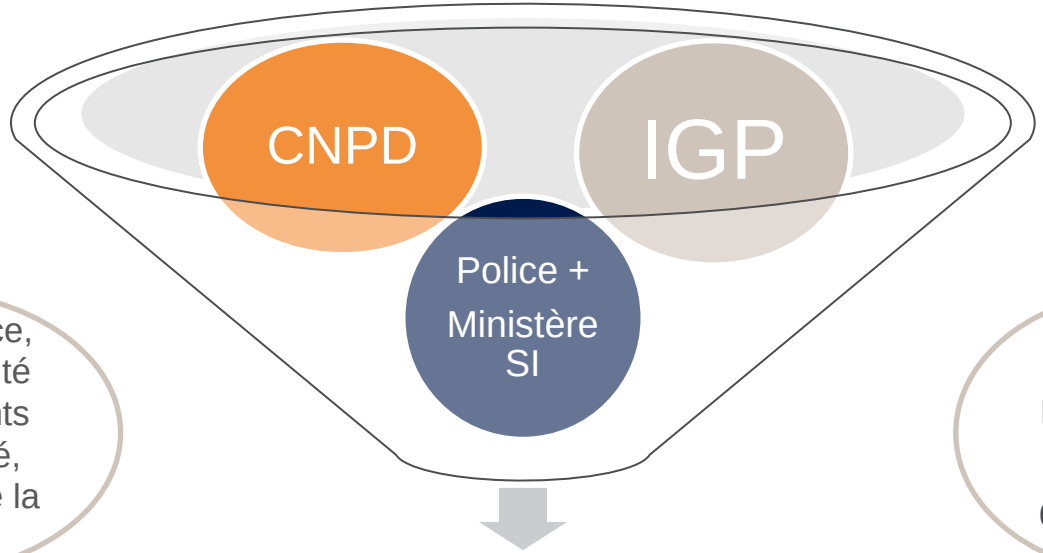
Nécessité de "précision législative"

- CEDH, Charte des droits fondamentaux et jurisprudence de la Cour Constitutionnelle
- Avis de la CNPD du 13 septembre 2019

***Benchmarking* des Etats voisins**

- Pays voisins ont une législation spécifique aux bases de données, surtout sur la base "centrale"
- mais variation au niveau de la précision, surtout pour les bases de données plus spécifiques

Mises en balance à opérer dans le dispositif législatif proposé



- Transparence, proportionnalité des traitements
- Accessibilité, prévisibilité de la loi

Flexibilité, réactivité et efficacité de la Police

Prise en compte dans les projets de loi et de RGD et décisions à venir

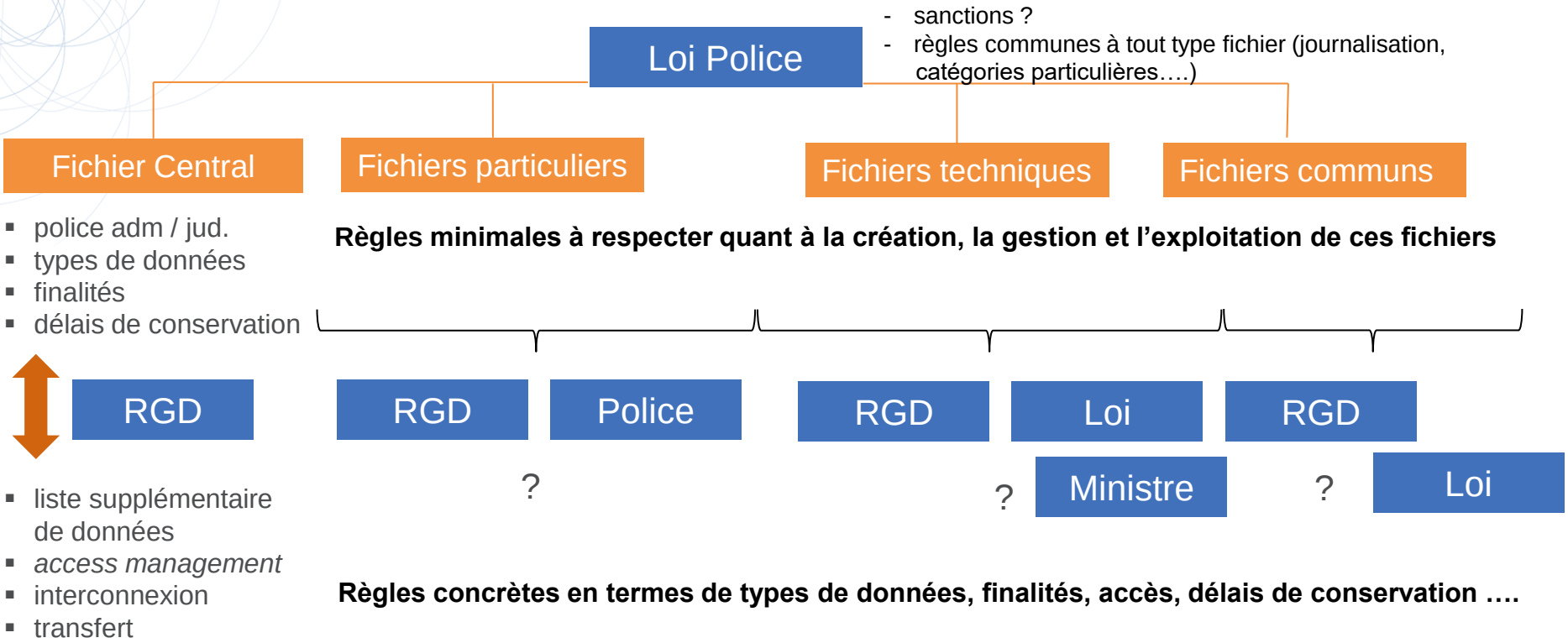
Proposition de catégorisation des fichiers (1)

Catégorisation proposée	Présentation sommaire	Exemple(s) / hypothèse(s)
Fichier central	▪ base centrale avec sous-division entre une partie "administrative'" et une partie "judiciaire" ▪ réglé par une loi avec des RGD d'exécution	N/A
Fichiers particuliers	(1) centralisation dans le fichier central = excessif / non-pertinent; ou (2) impossibilité technique d'alimenter le fichier central. Une loi définit les règles de base pour la création des bases de données. Les fichiers concrets sont réglés par RGD ou peuvent être déterminés à un niveau de la direction concernée de la police (DG/DCPA/DCPJ)*, mais sont soumis à l'avis du DPO, MSI et en principe à celui de la CNPD. *~Belgique + bases de données *ad hoc* en France concernant gilets jaunes	- "AFIS" pour la gestion des empreintes digitales. - "API (*Advanced Passenger Information*)" pour le contrôle des voyageurs.

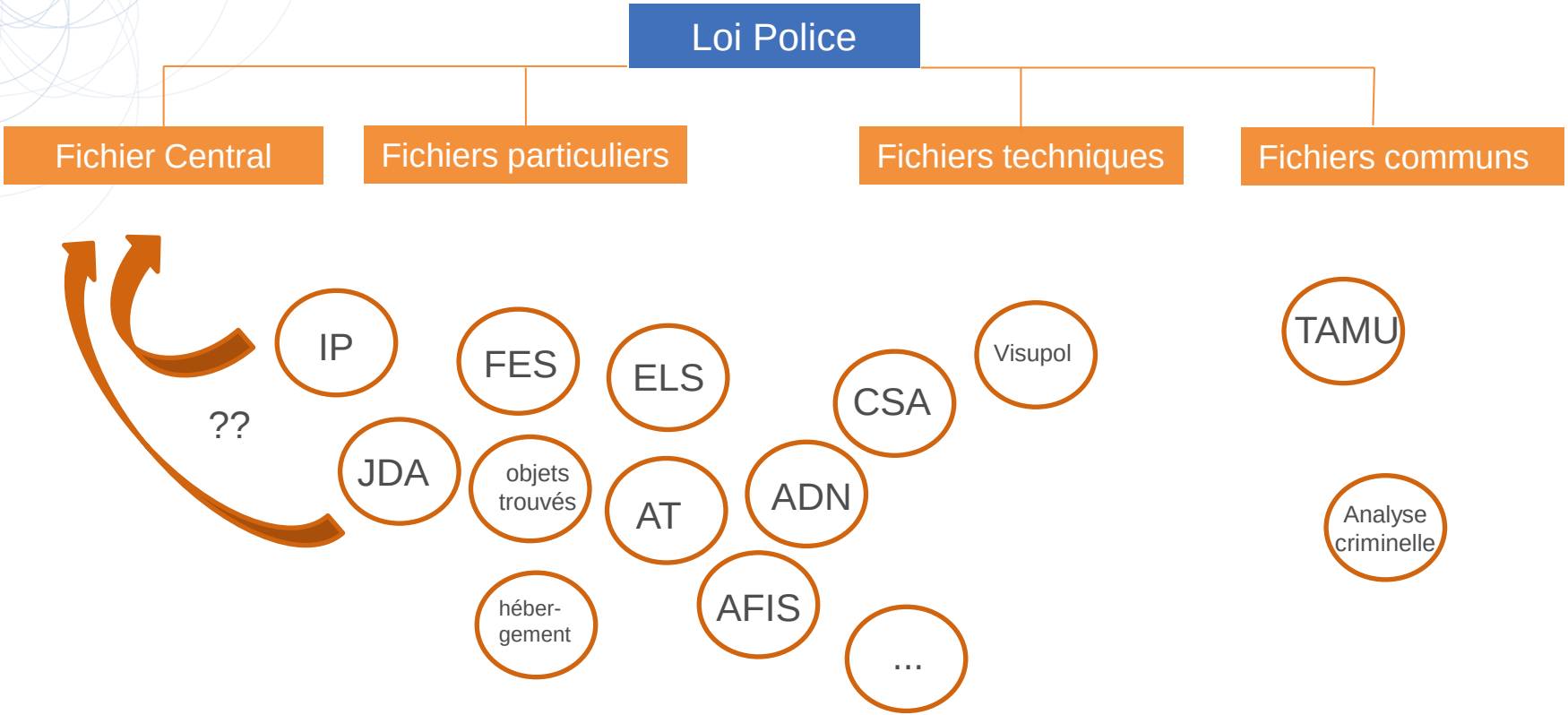
Proposition de catégorisation des fichiers (2)

Catégorisation proposée	Présentation sommaire	Exemple(s) / hypothèse(s)
Fichiers techniques	(1) fichiers de nature technique; et (2) issus d'outils techniques qui enregistrent automatiquement des données de manière structurée. Une loi définit les règles minimales à respecter quant à la création, la gestion et l'exploitation de ces fichiers. Les fichiers concrets sont réglés par loi, RGD ou peuvent être déterminés par le ministre, auquel cas ils sont soumis à l'avis du DPO et, en principe, à celui de la CNPD.	Système existant dit "CSA" (Loi modifiée du 25 juillet 2015) et utilisant des appareils de contrôle automatisé destinés à constater et à enregistrer les infractions à la législation routière.
Fichiers communs	▪ Fichiers de données issus de l'exercice conjoint de missions par différentes autorités, organes, organismes, services, direction ou commission. ▪ Fichiers avec plusieurs responsables du traitement. Une loi définit les règles minimales à respecter quant à la création, la gestion et l'exploitation de ces fichiers. Les fichiers concrets sont réglés par RGD et sont soumis à l'avis de la CNPD.	- Création/gestion conjointe d'une base de données par la Police et les autorités judiciaires (en Belgique, par exemple en matière de terrorisme, …). - Potentiellement le fichier dit "TAMU" (*Threat Assessment and Management Unit*)

Proposition de structure du nouveau dispositif législatif



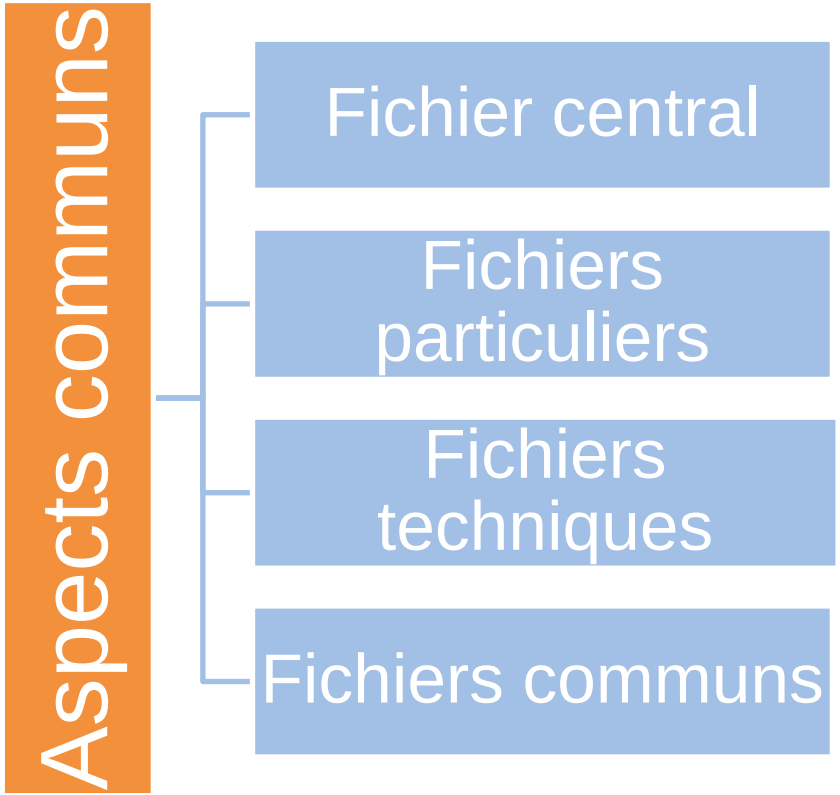
Proposition de structure du nouveau dispositif législatif



Transparence accrue surtout pour les aspects réglés par une décision du MSI ou de la Police (DG / DCPJ / DCPA)

1 Proposition pour la structure du nouveau dispositif législatif

2 Dispositions matérielles



éviter redondances avec L. 1.8.2018 mais concrétisation des principes

Aspects communs – cohérence re identification responsable du traitement

L. 1.8.2018 + Loi Police

- Police

RGD Avertissements taxés + L. vidéosurveillance

Directeur-général de la police

Aspects communs – droits des personnes concernées

L. 1.8.2018

+ spécifier quand l'accès aux données a lieu indirectement via la CNPD

mieux organiser la transparence / fourniture d'information

Aspects communs

Accès au fichier

- Principe "*need to know*" (aussi *split* PJ et PA)
- Détails à régler par type de fichier : qui fixe les droits d'accès, liste des catégories de personnes (OPJ & APJ, etc.) avec accès et catégories de données correspondantes
- Accès/interrogation directs
- Transfert de données
- Interconnexion

Journalisation

- Règles permettant la journalisation effective et précise:
  - Du motif de la consultation; et
  - De l'identité de la personne à l'origine de la consultation (aujourd'hui difficulté à retracer la personne dans certains cas)

Aspects communs – données sensibles / mineures

Garanties supplémentaires spécifiques pour données sensibles

Recherche suivant des critères relevant de données sensibles (actuellement impossible) sera interdite

Garanties pour toutes les données sensibles

Mesures de sécurité renforcées selon les cas

Recueil de données sensibles au sein d'informations douces strictement limité

Garanties pour les données de mineurs (prise en compte de loi 10 août 1992)

Délais de conservation des données réduits

Enregistrement que pour certaines infractions

Utilisation des données limitée à l'essentiel

Droit d'accès aux données restreints

Aspects communs - sanctions

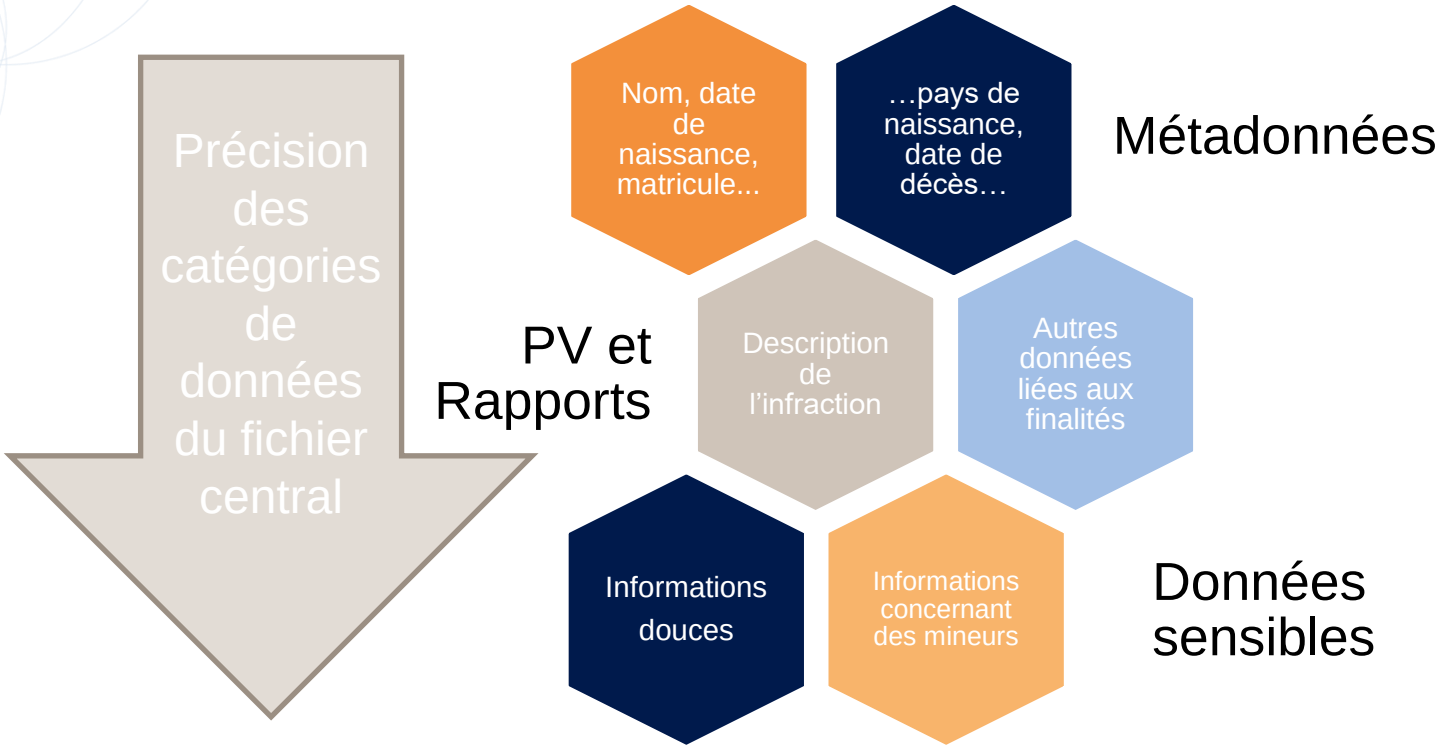
Violation principes clés

- non-respect droits d'accès ?
- traitement données sensibles
  - → intention spéciale

Violation missions policières

- sanction en cas de non-alimentation des fichiers pertinents ?
- (~Belgique – v. aussi principe d'exactitude de données !)

Fichier central



Fichier central

Distinction entre personnes concernées

(1) pour nouveaux dossiers

(2) dans les parties du fichier où réalisable

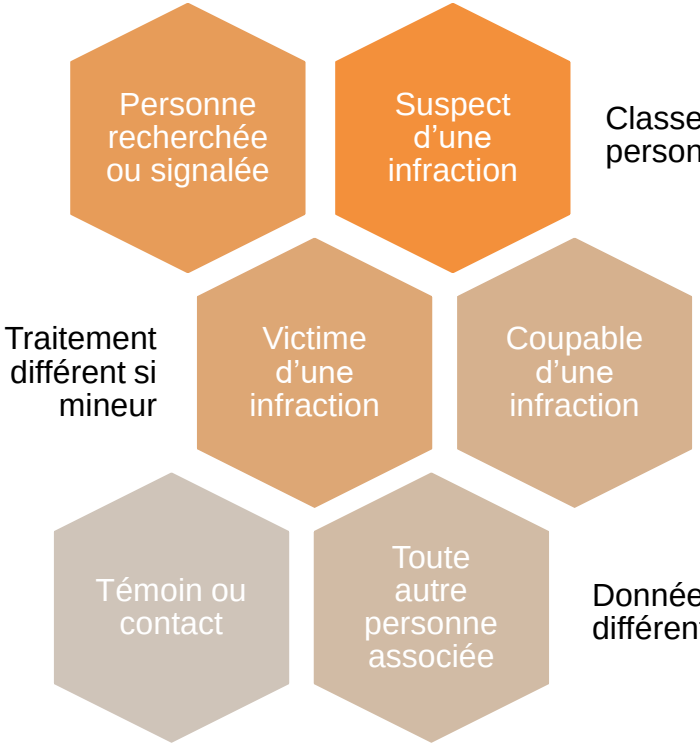
+

Plan de contrôle de la qualité des données basé sur le retour des autorités judiciaires

→

Qualité des données

Fichier central



Classement selon la qualité de personne concernée

Traitement différent si mineur

Données collectées différentes selon qualité

Fichier central

Critères de détermination des délais de conservation des données	- Issue d'une affaire (p. ex. acquittement) - Préservation des garanties des personnes en cas de révision - Retour des autorités judiciaires sur les suites données aux PV - La personne concernée par les données (p. ex. suspect, inculpé)
	- Expérience de terrain acquise par la Police - Flexibilité pour atteindre mission de la police (avis CNPD) - Objet du fichier (PA/PJ), nature et gravité des infractions et faits
	- Réduction des délais pour les informations douces - Allongement des délais dans cas préalablement définis (p. ex. reste une mesure à prendre sur base de décision d'une autorité) - Distinction conservation / archivage (procédure plus stricte d'accès comme c'est le cas maintenant)

Fichiers particuliers

Cas d'application	Règles concernant la création	Règles concernant la gestion et l'exploitation
Recours à des fichiers particuliers pour mêmes finalités servant aux missions de PJ ou de PA mais centralisation dans fichier central techniquement difficile ou inappropriée, notamment: • les différents FES; • bases de donnée ADN; • ELS ; • objets trouvés relatives à la recherche et la poursuite de crimes et délits; • ….	Procédure avant création de fichier par DCPJ ou DCPA (une création par loi ou RGD reste possible) : 1. demande un avis préalable du DPO; 2. joint une DPIA à sa demande au DPO si une DPIA est requise ; 3. analyse les éventuelles recommandations du DPO; et 4. demande d'avis préalable à la CNPD.	Loi du 1er août 2018 + règles minimales à respecter notamment: • délais de conservation; • profils et modalités d'accès aux données à déterminer sur base du principe *need to know* et des obligations de confidentialité; • détermination des règles d'interconnexion et de tous les destinataires de données; • garanties spécifiques en cas de traitement de données de mineurs.

Fichiers techniques

Cas d'application	Règles concernant la création	Règles concernant la gestion et l'exploitation
Recours à des fichiers techniques (collecte automatique + données techniques) dans des cas prévus par la loi à venir, par exemple dans le cadre du constat des infractions routières (p.ex. caméras intelligentes de reconnaissance des plaques comme en Belgique).	Procédure avant création de fichier par le Ministre (une création par loi ou RGD reste possible aussi): 1. demande un avis préalable du DPO; 2. joint un DPIA à sa demande au DPO; 3. analyse les éventuelles recommandations du DPO; et 4. demande d'avis préalable à la CNPD.	Loi du 1er août 2018 + règles minimales à respecter notamment: • définition des contrôles permettant une intervention humaine du responsable du traitement pour certains traitements automatisés; • délais de conservation; • profils et modalités d'accès aux données à déterminer sur base du besoin d'en connaître (*need to know*) et des obligations de confidentialité; • détermination des règles d'interconnexion et de tous les destinataires de données; • garanties spécifiques en cas de traitement de données de mineurs.

Dispositions matérielles de la nouvelle loi – Fichiers communs

Cas d'application	Règles concernant la création	Règles concernant la gestion et l'exploitation
• Création en Belgique dans le cadre de prévention et suivi du terrorisme (Loi sur le fonction de police + arrêté royal "Propagandiste de haine" d'avril 2018). • Au Luxembourg, certains fichiers sont sous la tutelle des autorités judiciaires mais nourris et utilisés par la police (ex. TAMU)→pas sûr si création et gestion conjointe *per se*. • A l'avenir, besoin pourrait exister pour création et gestion commune d'une base de données intégrée (rapidité, meilleur accès à l'information, mise à jour des données, etc.)	Procédure avant création de fichier: • les responsables du traitement **déclarent le fichier commun pour avis à la CNPD**; • **publié, après avis de la CNPD, par Loi / RDG**.	Loi du 1er août 2018 + règles minimales à respecter notamment: • un gestionnaire et un responsable opérationnel sont désignés pour chaque fichier commun sur proposition conjointe des responsables du traitement; • le gestionnaire est chargé de la gestion technique et fonctionnelle du fichier; • le responsable opérationnel est chargé de la gestion opérationnelle du fichier; • délais de conservation; • règles d'accès / interconnexion, détermination destinataires des données et garanties spécifiques pour mineurs.

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