



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Session ordinaire 2019-2020

MW/PR

P.V. SID 04
P.V. J 10

Commission de la Sécurité intérieure et de la Défense

Commission de la Justice

Procès-verbal de la réunion du 5 décembre 2019

Ordre du jour :

Présentation de l'étude réalisée par l'Inspection générale de la Police portant sur les traitements des données à caractère personnel dont le responsable de traitement est le directeur général de la Police

*

Présents : Mme Diane Adehm, Mme Semiray Ahmedova, Mme Nancy Arendt épouse Kemp, M. Carlo Back, M. Eugène Berger (en rempl. de M. André Bauler), M. Dan Biancalana, Mme Stéphanie Empain, M. Georges Engel, M. Marc Goergen, M. Gusty Graas, M. Max Hahn, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, 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. Marc Goergen, Mme Carole Hartmann, M. Charles Margue, Mme Octavie Modert, M. Laurent Mosar, Mme Lydie Polfer, M. Gilles Roth, membres de la Commission de la Justice

M. Marc Baum, observateur délégué

M. François Bausch, Ministre de la Sécurité intérieure
Mme Sam Tanson, Ministre de la Justice

Mme Béatrice Abondio, Direction, du Ministère de la Sécurité intérieure

Inspection générale de la Police :

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

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : M. Léon Gloden, membre de la Commission de la Sécurité intérieure et de la Défense

M. Franz Fayot, M. Léon Gloden, M. Roy Reding, membres de la Commission de la Justice

M. Henri Kox, Ministre délégué à la Sécurité intérieure

*

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

*

Présentation de l'étude réalisée par l'Inspection générale de la Police portant sur les traitements des données à caractère personnel dont le responsable de traitement est le directeur général de la Police

Monsieur le Ministre remercie vivement les membres de l'Inspection générale de la Police (IGP) pour l'étude détaillée sur les traitements des données à caractère personnel de la Police et remet un exemplaire à l'Administration parlementaire pour consultation, en demandant de ne pas en faire des copies ou d'en divulguer des éléments pour la raison que l'IGP a interviewé une soixantaine de membres de la Police et que l'étude contient des informations personnelles ou des informations permettant d'identifier l'auteur.

Les travaux continueront au Comité de suivi, mis en place en octobre 2019 au sein du ministère de la Sécurité intérieure, où sont en outre représentés la Police, la Justice, les autorités judiciaires, l'IGP et la CNPD. Les recommandations de celle-ci et de la Commission nationale pour la protection des données (CNPD) seront intégrées dans un tableau.

Le Gouvernement a mis à disposition de la Police les moyens budgétaires pour avoir recours à de l'aide externe pour la mise en œuvre informatique.

Madame l'Inspecteur général et Monsieur l'Inspecteur général adjoint présentent l'étude à l'aide d'un document PowerPoint en fournissant des précisions (cf. annexe).

- La portée et les limites de l'étude (p. 3)

La mission de l'IGP consistait à établir un état exhaustif des traitements dont le directeur général de la Police est le responsable de traitement. En raison du grand nombre de traitements, l'accent a été mis sur ceux qui sont de nature policière ou judiciaire, par rapport à ceux qui sont de nature purement administrative.

L'étude a insisté sur trois dimensions :

- la qualité des données
- leur durée de conservation
- l'accès aux données.

L'étude présente aussi des limites :

- elle n'est pas de nature technique, comme la protection des données n'est pas un domaine dans lequel l'IGP travaille quotidiennement ; la mission de l'IGP consiste à contrôler le fonctionnement de la Police, tandis que la protection des données relève du domaine de compétence de la CNPD ; l'étude réalisée par l'IGP s'est fondée sur les principes de base des textes

- La Police est depuis deux ans en plein processus de mise en conformité de ses traitements de données et ce processus se poursuivra encore longtemps ; en outre, l'étude s'est faite sur un terrain en évolution permanente.

- La méthode utilisée (p. 4)

L'étude a utilisé deux sources : les documents et les entretiens semi-directifs.

- La contribution de l'IGP (p. 5)

L'étude consiste en

- un rapport transversal : l'une des missions ayant été de chercher le motif de la création des bases de données, leur base légale, les différents textes et sources ont été examinés dans une optique transversale ; l'analyse transversale des fichiers a abouti en treize conclusions générales ;

- 80 fiches signalétiques, une fiche par base de données ; ces fiches se fondent sur les informations contenues dans le registre des banques de données de la Police grand-ducale (désigné par l'IGP comme « DataReg »), à savoir les informations indiquées par la Police (base légale, inscription du traitement, finalité du traitement, le destinataire). L'IGP a ajouté en bas son appréciation (avantages-inconvénients) et les problèmes constatés ou ressentis, ces deux éléments résultant de l'analyse des documents et des entretiens semi-directifs.

- La structure du rapport (p. 8)

Ont été considérés :

- les trois exigences (protection de la vie privée – obligations de la coopération policière européenne et internationale – efficacité policière)

- l'évolution de la législation dont le règlement grand-ducal modifiée du 2 octobre 1992 relatif à la création et l'exploitation d'une banque de données nominatives de police générale (règlement INGEPOL)

- certains fichiers ou groupes de fichiers

- 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, transposant la directive 2016/680 du 27 avril 2016 en droit national

- la question des accès et des motifs de consultation.

- Enquête administrative de l'IGP dans l'univers INGEPOL (p. 9)

À côté de l'analyse de nombreux documents et avis, l'IGP a également déjà fait des enquêtes administratives, dont celle dans le cadre d'une réclamation en 2015 d'un citoyen verbalisé en 2013 pour excès de vitesse. Pour établir cette infraction, il faut retracer l'historique sur les trois dernières années ; or, les deux APJ (agents de police judiciaire) étaient remontés jusqu'en 1996. La réclamation a révélé de graves dysfonctionnements dans le traitement de données. Le règlement INGEPOL alors en vigueur réservait l'accès aux OPJ (officiers de police judiciaire). En outre, l'archivage était inexistant.

L'IGP a par la suite émis une série de recommandations qui sont toujours d'actualité ; ainsi, la Police a entamé en février 2016 l'archivage.

- Le registre dressé par la Police (p. 10)

Trois fichiers n'étaient pas répertoriés dans le registre.

- Les trois exigences (p. 11)

- La sensibilisation à la protection des données (p. 12)

Plusieurs constats ont été faits :

- Le policier utilise les fichiers sans trop se poser de questions au sujet de la protection de la vie privée.
- Il en va de même pour ceux qui sont chargés de la conception des programmes.

La recommandation 1 de l'IGP a par conséquent pour objet la sensibilisation des membres de la Police, aussi pour rassurer les policiers qui travaillent avec les fichiers.

- L'analyse de divers fichiers ou groupes de fichiers (p. 13-25)

Le premier est le **fichier central**, où l'IGP reprend aussi les recommandations de la CNPD, voire va plus loin.

Se pose la question du « retour judiciaire », lequel se rapporte au futur ; or, que se passe-t-il avec les données contenues actuellement dans le fichier central, qui n'ont pas encore atteint la durée de conservation de dix ans ?

Par ailleurs, le fichier central contient aussi des données relatives aux missions de police administrative (déterminées par la loi modifiée du 18 juillet 2018 sur la Police grand-ducale), ce qui va à l'encontre d'une certaine homogénéité des données ; ainsi, le terme de PESAPI (personne susceptible d'avoir participé à une infraction pénale) n'est pas transposable dans le domaine de la police administrative.

Se pose encore la question du fichier des affaires archivées ; après 10 ans de conservation au fichier central, les procès-verbaux et autres données sont archivés. L'archivage est en quelque sorte une occultation du procès-verbal, puisque celui-ci n'est pas transféré dans un fichier propre.

Les trois recommandations de l'IGP concernant le fichier central se lisent comme suit :

Recommandation 2

Alors que le retour informatisé du suivi judiciaire a pris effet récemment et qu'il ne porte que pour les procès-verbaux et rapports judiciaires futurs, l'IGP recommande à la Police de ne pas négliger les données contenues dans le fichier central non visées par ce retour et de procéder, de concert avec les autorités judiciaires, à une vérification au cas par cas desdites données quant à leur validité et à leur exactitude.

Recommandation 3

Sous réserve de problèmes techniques majeurs, les documents archivés devraient être versés dans un fichier spécifique.

Recommandation 4

Les rapports dressés dans le cadre des missions de police administrative de la Police devraient faire l'objet d'un fichier dédié à cette matière.

Les **fichiers d'enquête spéciale (FES)** sont liés chacun à un type d'enquête spécifique. (p. 15)

Le problème que rencontrent ces fichiers tient à l'enregistrement dans ces fichiers d'informations douces (données sans consistance judiciaire, par exemple une rumeur) et d'informations solides.

L'importance de ces fichiers pour la Police est incontestable, mais il faut veiller à la qualité des informations.

Recommandation 5

(Concernant les FES) Alors que ce type d'informations suscite maintes interrogations quant à leur fiabilité et quant au droit au respect de la vie privée, il importerait que la Police se dote d'une méthode de contrôle de leur qualité, qu'elle détermine les critères entourant l'insertion de données dites douces dans les fichiers de police.

Elle pourrait s'inspirer pour ce faire de la grille d'évaluation reprise à l'article 29 du règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à Europol. Elle devrait également, conformément à l'article 6, paragraphe 1^{er} de 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 intérieure, opérer une distinction entre les données à caractère personnel fondées sur des faits et celles fondées sur des appréciations personnelles.

L'ELS (Einsatzleitsystem) permet de faire intervenir les patrouilles avec une efficacité maximale.

La suppression du Journal des incidents (JDI), plutôt en raison d'abus que pour inefficacité, laisse un grand vide informationnel pour le policier sur le terrain qui n'a plus connaissance des incidents ayant eu lieu avant le début de son service. Ce vide doit être comblé, aussi pour la sécurité du citoyen.

Recommandation 6

Le déficit informationnel devrait être comblé par la mise en place d'un autre outil. Dans la conception de celui-ci, il pourrait être opportun de s'orienter en fonction des suggestions émises par l'ancienne autorité de contrôle « article 17 ».

Le **Journal des affaires (JDA)** (p. 18) a pour objet d'organiser la gestion des écrits judiciaires. Cet instrument est destiné à garantir la transparence dans un dossier judiciaire, notamment en donnant un numéro de série aux documents, ce qui est aussi utile à la défense du concerné.

La qualité dépend des données enregistrées par l'enquêteur. Le système, développé par un informaticien de la Police il y a une vingtaine d'années, ne permet cependant pas de soustraire un dossier, ce qui est problématique quant à la durée de conservation des données. La Police en a conscience et un nouveau JDA semble être en cours d'élaboration.

Pour ce qui est des **fichiers liés aux avertissements taxés (AT)**, l'autorisation pour la création d'un tel fichier en général était prévue par le 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. La base légale de ce règlement fut la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Pour les AT générés par le Service de sanction et de contrôle automatisés (SCSA), la création est prévue par le règlement grand-ducal du 7 août 2015 autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de

contrôle et de sanction automatisés qui a deux bases légales : la loi précitée du 2 août 2002 et la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques.

La loi précitée du 1^{er} août 2018 a remplacé la loi précitée du 2 août 2002, de sorte que le règlement grand-ducal précité du 21 décembre 2004, qui prévoyait l'accès de l'IGP au fichier pour contrôle, n'existe plus. La Police est en train de remplacer ce règlement grand-ducal par des prescriptions de service. L'IGP rend attentif au danger de substitution d'un règlement grand-ducal par des prescriptions de service et constate que son rôle n'est pas repris par le projet de prescription de service. L'IGP dispose cependant en vertu de l'article 6, alinéa 1^{er} de la loi du 18 juillet 2018 sur l'Inspection générale de la Police d'un pouvoir de contrôle : « L'IGP procède, de manière systématique ou périodique, d'office ou sur demande du ministre, à des opérations de contrôle thématiques portant sur certaines activités de la Police. ».

L'IGP contrôle chaque année notamment l'annulation et la destruction d'AT.

Comme le règlement grand-ducal précité du 21 décembre 2004 ne concerne pas seulement la Police, l'IGP fait la suggestion que « Le principe devrait être arrêté que toute banque de données intéressant plusieurs ministères et administrations, hors l'autorité de contrôle prévue à la loi du 1^{er} août 2018, devrait être régie[s] par un règlement grand-ducal et non par une prescription de service. »

Par ailleurs, le fichier AT concerne également les AT pour les infractions à la loi anti-tabac, à la loi sur la pêche et autres. L'IGP s'interroge si une catégorisation n'est pas préférable à un fichier fourre-tout.

Au sujet de la durée de conservation, l'IGP fait la recommandation suivante :

Recommandation 7

Comme la Commission de la Sécurité intérieure et de la Défense de la Chambre des Députés en a exprimé le souhait, il y aurait lieu de fixer la durée de conservation des données personnelles en rapport avec des contraventions mineures au Code de la Route à un an, à compter du jour du paiement de l'avertissement-taxé y relatif ou de la transmission du procès-verbal afférent aux autorités judiciaires.

Pour les contraventions graves au Code de la Route, tel le délit de grande vitesse (dont un élément constitutif est la récidive dans un délai de 3 ans), la durée de conservation des données personnelles sera de 3 ans, à compter du jour où la condamnation précédente pour le même fait sera devenue irrévocable ou du jour où l'intéressé se sera acquitté de l'avertissement-taxé.

Les fichiers de police scientifique (p. 23) sont :

- le fichier ADN, basé sur la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle ; cette loi pose un cadre strict pour le traitement de données et contient déjà un grand nombre d'éléments de protection des données, s'inspirant du système français
- le fichier AFIS (Automated Fingerprint Identification System - Système d'identification automatique par empreintes digitales)
- le fichier STARLIMS, qui existe depuis janvier 2019, est d'une grande importance en matière de traces (gestion de la collecte, du traitement, du stockage, de la recherche et de

l'analyse des informations générées au laboratoire de police scientifique du Service de Police judiciaire (SPJ)

Recommandation 9

Plus généralement, le problème de la conservation des données personnelles dans des fichiers judiciaires se pose avec acuité.

Pour bon nombre de bases de données, les annulations ou effacements n'ont pas lieu. L'IGP a constaté que les agents ne procèdent à aucune annulation de données sans ordonnance de la part des autorités judiciaires ou instructions de la hiérarchie. Par conséquent, il n'est pas à exclure que des données figurent dans les bases de données alors qu'elles ne doivent plus y figurer. Un suivi rigoureux en la matière de la part des instances compétentes permettrait de tenir à jour les bases de données.

Au niveau de la base de données traitant les profils ADN se pose un problème particulier étant donné qu'à l'heure actuelle seul le profil ADN est effacé tandis que les données personnelles et les condamnations ne le sont pas. En effet, il semble peu clair aux agents quelles sont les données à effacer dans ce contexte.

À une question générale de M. Laurent Mosar (CSV) sur la durée de conservation des données après le décès d'une personne, Madame l'Inspecteur général répond que la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle prévoit à l'article 7, paragraphe 1^{er} :

« (1) Un profil d'ADN ayant pu être attribué à une personne déterminée ainsi que les informations y relatives peuvent faire l'objet du traitement ADN criminalistique jusqu'au jour où:

1. la personne à laquelle il se rapporte a été acquittée, par une décision judiciaire coulée en force de chose jugée, pour les faits ayant donné lieu à l'établissement de son profil d'ADN, ou
2. les faits ayant donné lieu à l'établissement du profil d'ADN en cause sont prescrits, ou
3. un délai de 10 ans s'est écoulé après le décès de cette personne. ».

M. Gilles Roth (CSV) estime que si une personne ne figure plus au Registre national des personnes physiques (RNPP) suite à la déclaration de décès à la commune (avec certificat de décès), elle ne continue pas à figurer dans un fichier judiciaire, son passé judiciaire devrait être effacé. L'orateur voudrait en outre savoir si des AT payés sont encore conservés pendant 48 mois au fichier.

Madame la Ministre de la Justice donne à considérer que l'automatisme fait défaut pour les personnes qui avaient quitté le pays, puisqu'il n'y a pas d'information de leur décès.

Il se peut aussi qu'après le décès, des éléments soient découverts qui laissent présumer que le défunt était l'auteur d'une infraction.

Mme Lydie Polfer (DP) rappelle que l'action publique s'éteint par le décès du concerné. Il serait cependant inopportun d'effacer immédiatement toutes les données, puisqu'elles peuvent aussi prouver que le défunt n'était pas l'auteur.

Monsieur l'Inspecteur général adjoint renvoie à l'article 4 de 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 qui dispose au paragraphe 1^{er} que: « (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. ».

Madame l'Inspecteur général revient à la recommandation 9 qui précise que « Au niveau de la base de données traitant les profils ADN se pose un problème particulier étant donné qu'à l'heure actuelle seul le profil ADN est effacé tandis que les données personnelles et les condamnations ne le sont pas. En effet, il semble peu clair aux agents quelles sont les données à effacer dans ce contexte. ».

La loi ADN date de 2006, tandis que le fichier était en place en 2008. En vertu de l'article 7 de la loi précitée du 25 août 2006, l'effacement se fait 10 ans après le décès. En pratique, en l'absence d'ordonnance de la part des autorités judiciaires ou d'instruction de la hiérarchie, les agents effacent le profil ADN, mais les données personnelles (nom, etc.) sont conservées. Cela s'explique par le fait que dans beaucoup d'affaires, plusieurs personnes sont concernées. Si tout le profil d'une personne était effacé, il n'y aurait plus de traçabilité.

Un interlocuteur a rendu attentif au fait que les utilisateurs de la base de données LuxDNA, dont des APJ et des stagiaires, voient les noms des personnes qui y figurent. Une mesure proposée est la transformation du nom en code numérique. (p. 25)

À noter que seulement 9 personnes ont accès au fichier ADN et 3 personnes ont accès au fichier AFIS.

Quant au **fichier hébergement** (p. 21), les données doivent être effacées 72 heures après leur transmission, à moins que leur maintien soit nécessaire pour la prévention, la recherche ou la constatation d'une infraction, le délai de conservation étant alors d'un mois, hormis leur utilisation dans le cadre d'une enquête préliminaire ou d'une instruction judiciaire.

Recommandation 8

Afin d'éviter que la destruction prématurée d'une information contenue dans le fichier « hébergement » ait des effets négatifs dans le domaine des enquêtes pénales, il est recommandé de fixer une durée de conservation de 3 mois, sauf si les données contenues dans ce fichier sont utilisées dans le cadre d'une enquête préliminaire ou d'une instruction préparatoire auquel cas leur durée de conservation est illimitée.

Mme Diane Adehm (CSV) s'intéressant à la location AirBnB, dont il n'y a pas de trace, M. Roth fait savoir que certaines communes ont changé leur règlement, obligeant les gens à communiquer le nom des personnes logées à la commune et de payer la taxe de séjour. En même temps, la conformité du logement avec le règlement communal des bâtisses est contrôlée.

Mme Lydie Polfer propose de se pencher une fois avec le ministre des Classes moyennes sur la problématique du AirBnB.

- La qualité des données (p. 26)

Recommandation 10

Pour lui permettre de procéder au contrôle des données, quant à leur fiabilité, leur exactitude, leur adéquation, leur caractère actuel et leur pertinence, la Police devrait définir une approche en la matière. Cette approche indiquerait le mode d'articulation des différents niveaux de contrôle, l'action des contrôleurs de premier rang et celle des contrôleurs subséquents, la fréquence et les délais de vérification de ces données.

Une documentation adéquate du contrôle permettrait une traçabilité sans lacunes.

- Les règles d'accès et les motifs d'accès (pp. 27 et 28)

Recommandation 11

Alors que l'accès aux différents fichiers de la Police constitue un point récurrent de discussion, l'IGP plaide pour la prise en compte des besoins réels (need to know) et objectifs liés à une fonction déterminée pour arrêter si un membre du personnel de la Police peut ou non bénéficier de l'accès à un fichier précis.

L'indication de l'accès à certaines bases de données pourrait être précisée dans la fiche de poste tout en conservant à l'esprit que l'objectif à moyen terme devrait être d'établir un profil individuel automatisé pour chaque membre de la Police.

Toute exception à cette règle, même temporaire, devrait être subordonnée à une procédure de demande d'accès dans le cadre de laquelle le DPO émettrait un avis conforme, après due consultation du gestionnaire du fichier, et sur base duquel le directeur général de la Police déciderait d'accorder ou non l'accès.

Afin d'éviter la survenance de tout risque d'oubli en cas de changement d'affectation, il conviendrait de procéder à une automatisation de tous les accès.

Enfin, toute nouvelle affectation impliquant l'ouverture de nouveaux accès devrait entraîner une remise à zéro des accès accordés pour l'exercice de la fonction antérieure.

Recommandation 12

Alors que la consultation de base de données pour des raisons extra-professionnelles demeure un risque constant et réel, l'IGP recommande à la Police de prévoir une motivation reprenant des motifs prédéfinis pour le personnel consultant une banque de données dans l'exercice habituel de sa mission et une motivation plus circonstanciée pour la consultation de tout autre fichier.

Par ailleurs, dans le cas de consultation d'une banque de données faite à la demande d'un collègue de travail habilité ou non à procéder lui-même à cette consultation, il conviendrait d'indiquer l'identité dudit collègue et le motif invoqué à la base de sa demande.

M. Gilles Roth voudrait savoir si la consultation d'une banque de données est possible sous un autre nom que le sien et sans indiquer de critère ou en l'effaçant après.

L'IGP ne peut pas donner de réponse claire, parce qu'elle ne peut pas analyser chaque accès.

- Les structures de la Police grand-ducale (pp. 29 et 30)

Recommandation 13

Afin de rencontrer dans les meilleures conditions ses obligations en matière de contrôle de la qualité des données, la Police doit se doter, autour du Data Protection Officer (DPO), d'une structure adéquate arrimée directement au directeur général de la Police.

Afin d'œuvrer à un meilleur continuum décisionnel et à une gestion centralisée en matière d'accès, il conviendrait de regrouper le service « règles des accès » et le bureau mutation dans une même cellule qui ferait partie de la structure évoquée ci-dessus.

Remerciant l'IGP pour l'étude, M. Marc Goergen (Piraten) saluerait l'ajout d'une liste des log-files pour chaque banque de données, notamment pour connaître la durée de conservation des données de journalisation pour chaque fichier.

Se ralliant aux remerciements, M. Laurent Mosar se montre choqué de certaines conclusions et constats, par exemple que des annulations et effacements n'ont pas lieu tant qu'il n'y a pas d'ordonnance judiciaire ou d'instruction de la hiérarchie (recommandation 9).

De manière générale, l'orateur souhaiterait savoir dans quel délai les recommandations seront suivies, certaines n'ayant pas besoin d'une nouvelle loi, l'orateur insistant sur la recommandation 9.

Monsieur le Ministre précise qu'il avait formulé une demande précise à la CNPD et à l'IGP concernant leurs missions respectives en matière de fichiers de la Police. Les recommandations de l'IGP et de la CNPD sont complémentaires et chacune sera mise en œuvre.

Madame la Ministre de la Justice confirme que les recommandations qui n'ont pas besoin de loi sont suivies, les autorités judiciaires ayant déjà réalisé des travaux importants. Parallèlement, l'Autorité de contrôle judiciaire examine au plan interne ce qu'il y a à faire en plus.

Madame l'Inspecteur général signale que la recommandation 9 se rapporte aux fichiers de police scientifique, c'est dans ce contexte qu'il faut la voir.

Monsieur Mosar considère que le fonctionnement avec les ordonnances n'est pas clair et demande si une instruction des autorités judiciaires est suffisante ou si une base légale devrait être créée.

Madame l'Inspecteur général rappelle la loi précitée du 25 août 2006, laquelle pose un cadre très strict et contient déjà un grand nombre d'éléments de la protection des données. Certains points sont encore à voir, la voie légale étant appropriée, l'oratrice signalant qu'il s'agit de banques de données des autorités judiciaires et alimentées par la Police.

Au sujet de l'archivage, est-ce que l'IGP est d'avis qu'un certain archivage devrait être maintenu ou doit-il être abandonné entièrement, comme semble le préférer la direction générale de la Police ?

L'IGP précise avoir réalisé l'étude avec les réalités du moment, mais estime que l'archivage pourrait être abandonné.

M. Marc Baum (déi Lénk) revient à l'enquête administrative de l'IGP dans l'univers INGEPOL et le cas concret du citoyen verbalisé en 2013 pour excès de vitesse, ce cas ayant révélé de graves dysfonctionnements. L'orateur voudrait savoir à qui se sont adressées les recommandations que l'IGP a ensuite émises et qui sont toujours d'actualité et quel en était le suivi.

Madame l'Inspecteur général souligne que les dysfonctionnements se situaient dans le passé. L'IGP indique dans son étude que les accès illégaux avaient lieu sur ordre du directeur général de l'époque.

Quand une enquête administrative est terminée, l'IGP envoie sa recommandation pour compte-rendu au ministre et une copie à la direction générale de la Police. L'oratrice précise que la nouvelle direction générale de la Police a tout de suite fait preuve d'une volonté claire

de se mettre en conformité avec l'article 2(1)2° du règlement grand-ducal modifié du 2 octobre 1992 relatif à la création et l'exploitation d'une banque de données nominatives de police générale (note de service du 27 novembre 2015). L'accès des APJ à la partie documentaire du fichier central a immédiatement été supprimé et les règles d'accès aux parties recherche et documentaire du fichier central ont été définies le 15 décembre 2015. De même, l'étude constate qu'en ce qui concerne le contenu des fichiers, la première avancée notable s'est faite le 4 février 2016 avec la publication d'une note de service concernant l'archivage de la partie documentaire du fichier central qui prévoyait que « les données de la partie documentaire datant de plus de 10 ans seront transférées à partir de mi-février 2016 vers la partie « ARCHIVES » ». Comme mentionné au début de la présentation, la Police fait déjà des démarches depuis deux ans.

En réponse à des critiques formulées par M. Roth, Monsieur le Ministre assure que rien n'est caché. Au contraire, la Police a reçu l'ordre de livrer tout ce qui est demandé et de répondre ouvertement à toutes les questions.

Madame l'Inspecteur général apporte une clarification au sujet du fichier des avertissements taxés. Les AT payés n'ont pas de suite. Pour les AT qui ne sont pas payés, un procès-verbal est dressé. Le fichier central contient entre autres les procès-verbaux, mais on ne peut pas dire de ce fait que les AT se trouvent au fichier central.

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

Procès-verbal approuvé et certifié exact

Annexe : Présentation de l'étude sur les fichiers de la Police

Présentation destinée à la
commission jointe « sécurité
intérieure et défense » et « justice »
de la Chambre des Députés
5 décembre 2019



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Sécurité intérieure

Inspection générale de la police

Etude sur les fichiers de la Police

- La portée et les limites de l'étude**
- La méthode utilisée**
- Les trois exigences**
- L'analyse de divers fichiers ou groupes de fichiers**
 - **Le fichier central**
 - **Les fichiers d'enquête spéciale**
 - **L'ELS**
 - **Le JDA**
 - **Les fichiers liés aux avertissements-taxés**
 - **Les fichiers de police scientifique**
 - **Le fichier hébergement**
- La qualité des données**
- Les règles d'accès et les motifs d'accès**
- Les structures de la Police grand-ducale**
- Conclusions**

La portée et les limites de l'étude

- ❑ Tous les fichiers dont le responsable de traitement est le DGP ont été considérés mais un accent particulier a été mis sur les fichiers de nature policière ou judiciaire par rapport aux fichiers purement administratifs
- ❑ Insistance sur trois dimensions :
 - La qualité des données
 - La durée de conservation des données
 - L'accès aux données
- ❑ Les limites :
 - L'étude de l'IGP n'est pas de nature technique
 - La Police est engagé depuis deux ans dans un vaste processus de mise en conformité de ses banques de données
 - Cette entreprise certes bien engagée est loin d'être terminée
 - Il est difficile de faire une étude dans de telles conditions sur un terrain en évolution permanente et où demeurent certaines incertitudes liées au processus de mise en conformité engagé par la Police

La méthode utilisée

- ▣ Pour la réalisation d'une étude, l'information est essentielle.
- ▣ **Deux sources :**
 - Les documents (outre les textes de loi et de règlements afférents, le registre des banques de données, les questions parlementaires, les travaux parlementaires, l'avis de l'autorité de contrôle « article 17 », l'avis de la CNPD, les prescriptions de service actuelles et celles projetées pour le futur, diverses archives et de très nombreuses pièces reçues de la Police)
 - Les entretiens semi-directifs effectués sur base de questionnaires homogènes en fonction de l'interlocuteur >>> une soixantaine d'interviews ont été réalisées auprès du personnel civil et policier actif dans le domaine étudié.

La contribution de l'IGP

- ▣ Un rapport transversal (voir ci-après)
- ▣ Une fiche signalétique par base de données comportant
 - La base légale
 - La description du traitement
 - La ou les finalité(s) du traitement
 - Etc

Ces informations sont reprises du registre des traitement établi par la PGD

- L'appréciation
- Les problèmes constatés ou ressentis (attention: pas toujours = aux recommandations)

Ces deux derniers éléments sont le fruit des constats tirés de l'analyse documentaire et des entretiens semi-directifs.

Exemples de fiches



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Sécurité Intérieure

Inspection générale de la police

PG-Rat (Fichier AT)

BASE LEGALE	DESCRIPTION DU TRAITEMENT	FINALITÉ DU TRAITEMENT	CATEGORIES DE DONNEES A CARACTÈRE PERSONNEL TRAITÉES
<p>loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques y compris la gestion des permis à points;</p> <p>autres lois spéciales où la procédure AT est prévue</p>	<p>banques de données des personnes ayant subi un avertissement taxé (AT)</p>	<p>recherche et de constatation d'une infraction punie d'une peine de police</p> <p>gestion administrative de la procédure de recouvrement et le cas échéant des poursuites judiciaires en cas de non-paiement</p>	<p>données des personnes concernées :</p> <ol style="list-style-type: none"> 1. nom(s) et prénom(s); 2. la matricule nationale; 3. date et lieu de naissance; 4. domicile, rue et numéro; 5. numéro d'immatriculation du véhicule ayant servi, le cas échéant, à commettre l'infraction; 6. numéro et pays de délivrance du permis de conduire; <p>données de l'agent verbalisant :</p> <ol style="list-style-type: none"> 1. nom(s) et prénom(s); 2. grade ; 3. codes d'identification ; 4. l'adresse courriel ;
PERSONNES AYANT ACCÈS	RESPONSABLE DU TRAITEMENT	DESTINATAIRES	DURÉE DE CONSERVATION
	<p>DG PGD Philippe SCHRANTZ</p>	<p>PGD</p>	<p>conservation dans l'application « Fichier AT » jusqu'à 48 mois après le paiement de l'AT 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 PV au Procureur d'Etat territorialement compétent.</p> <p>Au-delà de cette période de 48 mois, les données en question peuvent uniquement être conservées sous forme dépersonnalisée.</p>

Appréciation

Il s'agit du fichier initié pour la recherche et la constatation des infractions au code de la route. Il couvre également la gestion administrative de la procédure de recouvrement ou de la procédure judiciaire.
Aucun problème identifié au niveau de l'utilisation du fichier, ce dernier est considéré comme opérationnel et utile.

Problèmes constatés

- Au niveau de la conservation des données, le règlement grand-ducal prévoit un délai de conservation de 2 ans deux ans tandis que le code de la route (Article 11 bis, 3ème paragraphe et Article 13, 2ème paragraphe) retient pour certaines contraventions graves des sanctions importantes en cas de récidive dans les 3 ans. Une modification du règlement grand-ducal s'impose donc en vue d'unifier les délais de conservation.
- La recherche et l'identification des propriétaires des plaques étrangères devraient être autorisées, actuellement cela n'est permis que dans le cadre des excès de vitesse (CSA).
- Le recouvrement des contraventions exige une implication très importante des officiers de police. Permettre aux communes de récolter ces sommes induirait un gain de temps pour les agents de la police.

Exemples de fiches



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Sécurité Intérieure

Inspection générale de la police

Hébergement

BASE LEGALE	DESCRIPTION DU TRAITEMENT	FINALITÉ DU TRAITEMENT	CATEGORIES DE DONNEES A CARACTÈRE PERSONNEL TRAITÉES
<p>article 45 de la Convention d'application des Accords de Schengen du 19 juin 1990 ;</p> <p>règlement grand-ducal du 5 août 2015 pris en application de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement</p>	<p>contrôle des voyageurs dans les établissements d'hébergement</p>	<p>Contrôle des voyageurs</p>	<p>nom et prénom(s)</p> <p>numéro de la pièce d'identité;</p> <p>date et lieu de naissance;</p> <p>code postal, localité et pays de résidence habituel (les indications de la rue et du numéro sont facultatives);</p> <p>nationalité;</p> <p>date d'arrivée;</p> <p>date présumée de départ;</p> <p>nombre total de personnes accompagnant le voyageur principal y compris tous les enfants et toutes les personnes voyageant en groupe;</p> <p>but du voyage: « affaires et congrès » ou « loisirs et autres ».</p>
PERSONNES AYANT ACCÈS	RESPONSABLE DU TRAITEMENT	DESTINATAIRES	DURÉE DE CONSERVATION
	<p>DG PGD Philippe SCHRANTZ</p>	<p>membres de la section "signalements nationaux et hébergement" et du bureau SIRENE de la DRI</p>	<p>effacement 72 heures après leur transmission, sauf si leur maintien est nécessaire pour la prévention, la recherche ou la constatation d'une infraction. Dans ce cas, et hormis leur utilisation dans le cadre d'une enquête préliminaire ou d'une instruction préparatoire, effacement au plus tard un mois après leur transmission.</p>

Appréciation

Avantages

- Le programme est moderne et facile à gérer.
- Les agents se montrent très satisfaits avec le fonctionnement du fichier qui repère régulièrement des personnes recherchées logeant dans des campings, auberges ou hôtels. En 2018, 64 personnes recherchées ont pu être retracées grâce à cette banque de données, chiffre avec une tendance croissante.

Inconvénients

- Les délais de conservation des données sont néanmoins jugés être trop courts. Les données des voyageurs sont, sauf exception, supprimées 72 heures après leur transmission à la police, souvent avant la fin du séjour des voyageurs dans la structure.

Problèmes constatés

- Il serait préférable que le délai des 72 heures ne commence à courir qu'à la sortie de la personne de la structure et non dès son arrivée.

Le rapport

Vue générale de sa structure

- Les trois exigences (protection de la vie privée – obligations de la coopération policière européenne et internationale – efficacité policière)
- Les interventions du législateur en la matière (de la loi du 31 mars 1979 à la loi actuelle sans omettre le règlement grand-ducal du 2 octobre 1992 avec l'affaire évoquée au slide suivant)
- L'analyse de certains fichiers ou groupes de fichiers
- Les exigences de la loi du 1^{er} août 2018 et de la directive 2016/680 (qualité de fiabilité des données, distinction des différentes personnes concernées, prise en compte des personnes vulnérables)
- La question des accès et des motifs de consultation

Enquête administrative de l'IGP dans l'univers INGEPOL

- ▣ réclamation en 2015 d'un citoyen verbalisé en 2013 pour excès de vitesse ;
- ▣ PV dressé par 2 APJ renseigne, outre les faits, « l'historique judiciaire » du citoyen en matière d'infractions au Code de la route de 1996 à 2013;

----- » Réclamation du citoyen a eu une portée bien plus large: révèle des dysfonctionnements graves en matière de traitements des données à caractère personnel au sein de la Police (critères d'accès non respectés, archivage inexistant...)

----- » L'IGP a émis des recommandations qui sont toujours d'actualité (archivage, échange d'informations automatisée avec autorités judiciaires, adaptation cadre légal, sensibilisation...)

Le registre dressé par la PGD

- ▣ Document essentiel pour la réalisation de l'étude

Constat :

Tous les fichiers ne sont pas répertoriés, il en manquerait trois, dont le fichier des dossiers disciplinaires des membres de la Police.

Les trois exigences

- ▣ Le respect de la vie privée consacré par la Convention européenne des Droits de l'Homme, par la Charte des droits fondamentaux de l'UE et par notre Constitution
- ▣ Le respect de nos engagements internationaux participant à la création d'un espace de liberté, de sécurité et de justice
- ▣ L'efficacité de l'action policière

La sensibilisation à la protection des données

- ❑ Le policier utilise les fichiers à sa disposition sans nécessairement se poser de questions !
- ❑ Les concepteurs réalisent les programmes qui leur sont demandés sans nécessairement se poser de questions !
- ❑ La dimension « protection des données » est le plus souvent absente !

Recommandation 1

Alors qu'il a été fait état à maintes reprises d'une certaine faiblesse en la matière, l'IGP recommande à la Police

- de mettre en place un plan ambitieux de sensibilisation de son personnel, du concepteur de programme à l'utilisateur final, aux principes régissant le domaine de la protection des données personnelles ;
- d'œuvrer à la prise en compte de ces principes dès la conception de tout traitement de données à caractère personnel.

L'analyse de divers fichiers ou groupes de fichiers

▣ Le fichier central

- Outil essentiel du travail policier
- En théorie trois fichiers
- L'appellation « fichier central » recouvre deux réalités :
 - ❖ Fichier ou ... fichier(s) et
 - ❖ moteur de recherche à l'aide de métadonnées
 - ❖ Lien avec d'autres fichiers ou le problème de la « recherche transparente »
- Le « retour judiciaire » est positif pour le futur
- mais qu'en est-il des procès-verbaux et rapports judiciaires insérés dans le FC quelques années avant la prise d'effet du « retour judiciaire » ?
- Le FC inclut également les rapports établis dans le cadre de l'exécution de missions de police administrative, ceci va à l'encontre d'une certaine homogénéité des données (le terme de PESAPI n'est pas transposable dans le domaine de la police administrative !)
- Qu'en est-il du fichier des affaires archivées ?

L'analyse de divers fichiers ou groupes de fichiers

Recommandation 2

Alors que le retour informatisé du suivi judiciaire a pris effet récemment et qu'il ne porte que pour les procès-verbaux et rapports judiciaires futurs, l'IGP recommande à la Police de ne pas négliger les informations contenues dans le fichier central non visées par ce retour et de procéder, de concert avec les autorités judiciaires, à la vérification des données introduites au fichier central avant ledit retour.

Recommandation 3

Sauf obstacle technique majeur, les documents archivés devraient être versés dans un fichier spécifique.

Recommandation 4

Les rapports dressés dans le cadre des missions de police administrative de la Police devraient faire l'objet d'un fichier dédié à cette matière.

L'analyse de divers fichiers ou groupes de fichiers

▣ Les fichiers d'enquête spéciale (FES)

- Il s'agit de fichiers liés à un type d'enquête spécifique
- Il en est ainsi du Fichier « stups », du fichier « Vols organisés », etc
- Certains sont actuellement régis par une prescription de service, d'autres effleurés, de troisième ne le sont pas du tout !
- Certains de ces fichiers ont été conçus par certains policiers et ont disparu avec l'affectation de ceux-ci à d'autres fonctions. Il en est ainsi du fichier « graffitis ».
- Ces diverses applications fonctionnent de manière autonome et sont gérées par la section concernée
- L'accès direct est généralement limité aux membres de la section du SPJ qui gère ce FES
- Sauf le fichier « STUPS » ... (exemple : CCPD)
- Ces fichiers sont essentiels mais....
- Les informations contenues dans les FES ne sont pas toutes consistantes >>>> informations douces
- **Problème au niveau de la qualité des données y insérées et de la durée de conservation**

L'analyse de divers fichiers ou groupes de fichiers

Recommandation 5

Alors que ce type d'informations suscite maintes interrogations quant à leur fiabilité et quant au droit au respect de la vie privée, il importerait que la Police se dote d'une méthode de contrôle de leur qualité, qu'elle détermine les critères entourant l'insertion de données dites douces dans les fichiers de police.

Elle pourrait s'inspirer pour ce faire de la grille d'évaluation reprise à l'article 29 du règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à Europol. Elle devrait également, conformément à l'article 6, paragraphe premier de 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 intérieure, opérer une distinction entre les données à caractère personnel fondées sur des faits et celles fondées sur des appréciations personnelles.

L'analyse de divers fichiers ou groupes de fichiers

▣ L'ELS

- Gestion optimale des patrouilles
- Très peu de texte libre mais des cases prédéfinies
- Les recherches y sont difficiles et peu prometteuses
- Pour le policier de terrain, l'absence du JDI laisse un grand vide informationnel
- Les défauts du JDI étaient surtout le fait de ses utilisateurs (remarques personnelles inappropriées, diffusion exagérée, etc)

Recommandation 6

Le déficit informationnel devrait être comblé par la mise en place d'un autre outil. Dans la conception de celui-ci, il pourrait être opportun de s'orienter en fonction des suggestions émises par l'ancienne autorité de contrôle « article 17 ».

L'analyse de divers fichiers ou groupes de fichiers

▣ Le JDA

- base de données qui a pour objet d'organiser la gestion des écrits judiciaires du Service de Police Judiciaire, de ses diverses antennes et des Services régionaux de Police spéciale ainsi que le suivi des devoirs judiciaires
- Le type de données varie en fonction de la qualité et de l'exhaustivité des informations enregistrées par l'enquêteur principal de l'affaire
- Le problème de la durée de conservation ; l'on ne peut en soustraire un dossier sous peine de mettre à mal tout le système !
- Mais un nouveau JDA est, paraît-il, en voie de gestation

L'analyse de divers fichiers ou groupes de fichiers

- Les fichiers liés aux avertissements-taxés
 - Initialement, le RGD de 2004 pour les AT en général mais sa seule base légale est la loi de 2002
 - Le RGD de 2015 pour les AT générés par le SCSA. Il a deux bases légales la loi de 2002 et la loi sur la SCSA
 - Avec la loi du 1^{er} août 2018 remplaçant la loi de 2002 >>> le RGD de 2004 n'existe plus or il prévoyait l'accès de l'IGP au fichier pour des raisons de contrôle. Le projet de PS ne prévoit plus explicitement cet accès >>> **danger de substitution d'un RGD par une PS.**
 - **Suggestion : Le principe devrait être arrêté que toute banque de données intéressant plusieurs ministères et administrations, hors l'autorité de contrôle prévue à la loi du 1^{er} août 2018, devrait être régies par un RGD et non par une prescription de service.**
 - **Constat : Par ailleurs, l'on constate que ce fichier concerne les AT pour infractions au Code de la Route, mais également pour des infractions à la loi anti-tabac, à la loi sur la pêche,... Est-ce souhaitable au niveau homogénéité des données ?**

L'analyse de divers fichiers ou groupes de fichiers

A propos du fichier « AT », il faudrait veiller à une approche plus ordonnée en matière de durée de conservation, d'où la recommandation suivante, **la recommandation 7** :

Comme la commission de la sécurité intérieure et de la défense de la Chambre des Députés en a exprimé le souhait, il y aurait lieu de fixer la durée de conservation des données personnelles en rapport avec des contraventions mineures au Code de la Route à un an, à compter du jour du paiement de l'avertissement-taxé y relatif ou de la transmission du procès-verbal afférent aux autorités judiciaires.

Pour les contraventions graves au Code de la Route, tel le délit de grande vitesse (dont un élément constitutif est la récidive dans un délai de 3 ans), la durée de conservation des données personnelles sera de 3 ans, à compter du jour où la condamnation précédente pour le même fait sera devenue irrévocable ou du jour où l'intéressé se sera acquitté de l'avertissement-taxé.

L'analyse de divers fichiers ou groupes de fichiers

▣ Le fichier hébergement

- Cette fiche est établie manuellement sur le support prévu à cet effet ou sous forme électronique. Le logeur communique à la Police grand-ducale la fiche d'hébergement en question.
- *« La Police grand-ducale traite les données recueillies dans un fichier temporaire. Ces données devront être effacées soixante-douze heures après leur transmission, à moins que leur maintien au-delà de ce délai ne soit nécessaire pour la prévention, la recherche ou la constatation d'une infraction. Dans ce cas, et hormis leur utilisation dans le cadre d'une enquête préliminaire ou d'une instruction préparatoire, les données doivent être effacées au plus tard un mois après leur transmission. »*

L'analyse de divers fichiers ou groupes de fichiers

Recommandation 8

Afin d'éviter que la destruction prématurée d'une information contenue dans le fichier « hébergement » ait des effets négatifs dans le domaine des enquêtes pénales, il est recommandé de fixer une durée de conservation de 3 mois, sauf si les données contenues dans ce fichier sont utilisées dans le cadre d'une enquête préliminaire ou d'une instruction préparatoire.

L'analyse de divers fichiers ou groupes de fichiers

- ▣ Les fichiers de police scientifique
- ▣ Il s'agit
 - du fichier ADN basé sur la loi du 25 août 2006,
 - du fichier AFIS portant sur les traces et empreintes et
 - du fichier STARLIMS qui porte lui sur la gestion de la collecte, du traitement, du stockage, de la recherche et de l'analyse des informations générées au laboratoire de la police scientifique du SPJ

L'analyse de divers fichiers ou groupes de fichiers

Recommandation 9

Plus généralement, le problème de la conservation des données personnelles dans des fichiers judiciaires se pose avec acuité.

Pour bon nombre de bases de données, les annulations ou effacements n'ont pas lieu. L'IGP a constaté que les agents ne procèdent à aucune annulation de données sans ordonnance de la part des autorités judiciaires ou instructions de la hiérarchie. Par conséquent, il n'est pas à exclure que des données figurent dans les bases de données alors qu'elles ne doivent plus y figurer. Un suivi rigoureux en la matière de la part des instances compétentes permettrait de tenir à jour les bases de données.

Au niveau de la base de données traitant les profils ADN se pose un problème particulier étant donné qu'à l'heure actuelle seul le profil ADN est effacé tandis que les données personnelles et les condamnations ne le sont pas. En effet, il semble peu clair aux agents quelles sont les données à effacer dans ce contexte.

L'analyse de divers fichiers ou groupes de fichiers

Autre constat

Un interlocuteur a souligné le fait que les utilisateurs (aussi stagiaires et APJ) de la base de données LuxDNA voient les noms des personnes y figurant. Une remise en question de ce état de choses, du moins en ce qui concerne les bases de données sensibles, n'a jamais été thématifiée à la Police.

Une mesure proposée dans ce contexte est de prévoir un code numérique permettant une anonymisation des données personnelles (prénom, nom). Cette pratique est déjà d'usage dans certaines administrations des pays limitrophes

A noter qu'une telle solution nécessiterait néanmoins des ressources personnelles supplémentaires auprès de la Police et au niveau du Parquet étant donné qu'une transformation du nom de la personne en code numérique et vice-versa serait nécessaire à un moment donné.

La qualité des données

- ▣ Rappelons que les données du fichier central et de certains fichiers d'enquête spéciale sont aussi consultées pour répondre aux demandes internationales (Europol, Interpol, CCPD).
- ▣ Cette exigence de qualité est omniprésente dans les textes de droit européen.

Recommandation 10

Pour lui permettre de procéder au contrôle des données, quant à leur fiabilité, leur exactitude, leur adéquation, leur caractère actuel et leur pertinence, la Police devrait définir une approche en la matière. Cette approche indiquerait le mode d'articulation des différents niveaux de contrôle, l'action des contrôleurs de premier rang et celle des contrôleurs subséquents, la fréquence et les délais de vérification de ces données.

Une documentation adéquate du contrôle permettrait une traçabilité sans lacunes.

Les règles d'accès et les motifs d'accès

Les efforts entrepris par la PGD en la matière doivent être salués !

Recommandation 11

Alors que l'accès aux différents fichiers de la Police constitue un point récurrent de discussion, l'IGP plaide pour la prise en compte des besoins réels (need to know) et objectifs liés à une fonction déterminée pour arrêter si un membre du personnel de la Police peut ou non bénéficier de l'accès à un fichier précis.

L'indication de l'accès à certaines bases de données pourrait être précisée dans la fiche de poste tout en conservant à l'esprit que l'objectif à moyen terme devrait être d'établir un profil individuel automatisé pour chaque membre de la Police.

Toute exception à cette règle, même temporaire, devrait être subordonnée à une procédure de demande d'accès dans le cadre de laquelle le DPO émettrait un avis conforme, après due consultation du gestionnaire du fichier, et sur base duquel le Directeur général de la Police déciderait d'accorder ou non l'accès.

Afin d'éviter la survenance de tout risque d'oubli en cas de changement d'affectation, il conviendrait de procéder à une automatisation de tous les accès.

Enfin, toute nouvelle affectation impliquant l'ouverture de nouveaux accès devrait entraîner une remise à zéro des accès accordés pour l'exercice de la fonction antérieure.

Les règles d'accès et les motifs d'accès

Recommandation 12

Alors que la consultation de base de données pour des raisons extra-professionnelles demeure un risque constant et réel, l'IGP recommande à Police de prévoir une motivation reprenant des motifs prédéfinis pour le personnel consultant une banque de données dans l'exercice habituel de sa mission et une motivation plus circonstanciée pour la consultation de tout autre fichier.

Par ailleurs, dans le cas de consultation d'une banque de données faite à la demande d'un collègue de travail habilité ou non à procéder lui-même à cette consultation, il conviendrait d'indiquer l'identité dudit collègue et le motif invoqué à la base de sa demande.

L'accès à certaines bases de données, notamment celles contenant des photographies de personnes, devrait également être subordonné à l'encodage d'un motif circonstancié.

Les structures de la Police grand-ducale

La place croissante prise par la protection des données implique

- la mobilisation des ressources humaines nécessaires et compétentes
- Un large degré d'indépendance organique
- Un arrimage au plus près du responsable de traitement, à savoir le DG
- Certains regroupements de services aux activités complémentaires

Recommandation 13

Afin de rencontrer dans les meilleures conditions ses obligations en matière de contrôle de la qualité des données, la Police doit se doter, autour du DPO, d'une structure adéquate arrimée directement au Directeur général de la Police.

Afin d'œuvrer à un meilleur continuum décisionnel et à une gestion centralisée en matière d'accès, il conviendrait de regrouper le service « règles des accès » et le bureau mutation dans une même cellule qui ferait partie de la structure évoquée ci-dessus.

Les structures de la Police grand-ducale

- ▣ Le recours à des sociétés privées est une solutions mais ...
- ▣ La présence de policiers ayant une longue expérience dans le domaine judiciaire serait très souhaitable
- ▣ Une piste : le recours à des retraités du SPJ !

Conclusions

- ▣ Divers constats ont été faits à propos desquels l'IGP ne formule pas nécessairement de recommandations
- ▣ 13 recommandations ont été formulées
- ▣ L'IGP partagent l'esprit de celles émises par le CNPD dans sa délibération n°45/2019 du 13 septembre 2019