TABLE DES MATIÈRES

RAPPORT ÉTABLI DANS LE CADRE DE L'ENQUÊTE DE CONTRÔLE RELATIVE AUX ACCÈS ILLÉGITIMES AUX BANQUES DE DONNÉES PAR LES MEMBRES DES SERVICES DE POLICE[1]

1. INTRODUCTION GÉNÉRALE

1.1. Problématique et contexte général

1. Dans son rapport annuel 2005, le Comité permanent P, après avoir déjà attiré auparavant l'attention sur cette problématique, relevait l'existence d'indices dénotant un possible estompement de la norme au sein des services de police en relation avec l'usage abusif des bases de données mises à leur disposition[2]. En 2009, le Comité permanent P relevait à nouveau que certains membres de la police semblaient continuer à abuser de leur accès à des données à des fins personnelles tant dans les banques de données policières que dans les banques de données externes auxquelles ils ont accès par leur fonction, comme le registre national ou le registre des véhicules immatriculés[3]. Dans ce contexte, le Comité permanent P a recommandé un ensemble de bonnes pratiques et invité la direction des services de police à sensibiliser et informer leur personnel. Cette recommandation a été rappelée dans le rapport annuel 2010[4].

2. Les possibles atteintes à la protection de la vie privée par les membres des services de police, droit garanti par la Constitution, entrent directement dans les préoccupations du Comité P en vertu de ses missions légales. Un premier examen (plus) approfondi de la situation a été effectué dans le cadre du rapport annuel 2013 approuvé par la Commission parlementaire de suivi le 7 janvier 2015.

---

[1] Dossier n°21530/2015.

[2] Rapport d'activités 2005 du Comité permanent de contrôle des services de police, *Doc. Parl.*, Chambre, 2006-2007, n° 3112/001 et Sénat, 2006-2007, n° 3-2410/1, pp. 53 à 57.

[3] Rapport d'activités 2009 du Comité permanent de contrôle des services de police, *Doc. Parl.*, Chambre, 2010-2011, n° 1165/001 et Sénat, 2010-2011, n° 5-754/1, pp. 71 et 72

[4] Cette recommandation prévoyait que « *Tout collaborateur de police qui cherche des informations dans des banques de données utilise uniquement son 'login' et son mot de passe personnels, enregistre le motif de chaque consultation comme le prévoit le règlement, et ferme toujours l'accès aux banques de données après chaque consultation. La direction devrait régulièrement rappeler ces règles aux collaborateurs et souligner le fait que des contrôles sont effectués dans ce sens. Il est également recommandé que les collaborateurs de police n'effectuent pas eux-mêmes des recherches dans la base de données à propos d'un membre de leur famille ou d'un ami dans l'exercice de leurs missions.* ».

Tableau 1 : Atteintes à la vie privée relevées en 2013 (Nombre d'allégations)[5]

Nature des allégations d'atteintes à la vie privée	2013	%	Dysfonct. établis	%
Accès illégitime aux banques de données	126	72,41%	64	36,78%
Autres formes d'atteintes à la vie privée	48	27.59%	11	6,31%
Total	174	100,00%	75	43,09%

Source : Base de données du Comité P

3. À cette occasion, il a été constaté que 72,41% des allégations visant de possibles atteintes à la vie privée lors de plaintes ou dénonciations enregistrées en 2013 dans la base de données du Comité P concernaient des accès illégitimes à des banques de données. Un dysfonctionnement a été établi pour 36,78% de ces allégations. Les autres formes d'atteintes à la vie privée relevées étaient essentiellement des diffusions illégitimes d'informations ainsi que le recueil ou l'archivage illégitime d'informations.

Tableau 2 : Dossiers enregistrés au Comité P dans le cadre de la fonctionnalité « banque de données » (Nombre de dossiers)[6]

Dossiers ayant trait à des banques de données	2012	2013	2014	2015
	148	138	84	83

Source : Base de données du Comité P

4. À titre indicatif, le nombre de dossiers enregistrés dans le cadre de la fonctionnalité « banque de données » connaît une diminution de 43,91% sur la période 2012-2015.

1.2. But de l'enquête

5. Face à la persistance d'accès illégitimes aux banques de données, le Comité permanent P a décidé d'ouvrir une enquête de contrôle visant, notamment, à mieux connaître les raisons pour lesquelles les consultations illégitimes continuent à se perpétuer et à examiner la manière dont s'exercent la prévention et la répression en la matière. Le champ des investigations a été limité aux accès aux banques de données les plus couramment utilisées par les membres des services de police lors de l'exercice de leurs activités. L'objectif poursuivi est de formuler des recommandations susceptibles d'aboutir à une amélioration notable de la situation.

[5] L'analyse des dossiers 2013 relatifs aux atteintes à la vie privée enregistrés dans la base de données du Comité P a été effectuée en examinant ceux-ci minutieusement un par un. À cette occasion, c'est l'allégation d'atteinte à la vie privée qui a servi de base de comptage, un dossier pouvant contenir plusieurs allégations d'atteinte à la vie privée différentes. Compte tenu du temps conséquent exigé par ce type d'analyse, il n'a pas été procédé à l'examen des dossiers 2012 et 2014 pour obtenir une tendance.

[6] Les dossiers enregistrés dans le cadre de la fonctionnalité « banque de données » sont pour la plus grande part des dossiers relatifs à des accès illégitimes aux banques de données.

1.3. Devoirs effectués

6. Les renseignements nécessaires concernant l'information et la sensibilisation des membres des service de police, la procédure de détection des abus aux banques de données, la procédure d'octroi des autorisations d'accès et le projet de directive régissant l'accès, l'utilisation et le contrôle des moyens ICT ont été recueillis au sein de la police fédérale. Pour ce faire, la Direction de l'information policière et des moyens ICT ('*Information and Communication Technology'*) (ci-après dénommée DRI) et le service « Sécurité de l'information et vie privée » ont, notamment, été consultés. Les données émanant de la banque de données jurisprudence du Conseil de discipline ont été exploitées afin de compléter la connaissance du phénomène. Les chefs de corps de trois zones de police locale ont également été consultés afin d'obtenir un aperçu de la manière selon laquelle le contrôle en la matière était pratiquement et concrètement exécuté. Le président de l'Organe de contrôle de l'information policière, la commissaire générale de la police fédérale ainsi que le président de la Commission permanente de la police locale ont été invités à faire connaître leurs commentaires et réactions sur base du projet de rapport d'enquête de contrôle.

1.4. Structure du rapport

7. Le rapport aborde successivement les modalités d'accès des membres des services de police aux banques de données, les mesures prises en vue de prévenir les abus, un aperçu des dysfonctionnements relevés et de leur répression, les difficultés rencontrées en matière d'établissement des abus, les raisons de la persistance des accès illégitimes, les pistes de réflexion en vue de lutter plus efficacement contre ceux-ci et la formulation de conclusions et de recommandations concrètes. Il se termine par l'examen des réactions des parties prenantes consultées et par les commentaires finaux du Comité permanent P.

2. CONSTATATIONS

2.1. Accès aux banques de données par les services de police

2.1.1. Cadre normatif

8. En vertu de l'article 44/1, §1er, de la loi du 5 août 1992 sur la fonction de police[7] (ci-après dénommée LFP), les services de police peuvent traiter des informations et des données à caractère personnel dans le cadre de l'exercice de leurs missions de police administrative et de police judiciaire pour autant que ces dernières présentent un caractère adéquat, pertinent et non excessif au regard des finalités de police administrative et de police judiciaire pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement. L'article 44/4 § 2. précise quant à lui que les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directives les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la loi. Au niveau européen, un règlement a été

[7] (*M.B.* du 22 décembre 1992).

récemment édicté en matière protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[8].

9. La directive ministérielle MFO-3[9] détaille, notamment, les modalités d'accès et de consultation des banques de données accessibles aux membres des services de police.

10. Les articles 54 à 56 du Code de déontologie des services de police[10] rappellent aux membres de services de police les règles relatives au respect de la vie privée et au recueil, à la gestion et à la consultation des informations. La transgression de ces règles peut donner lieu à des sanctions disciplinaires.

11. Sur le plan pénal, un certain nombre d'infractions sont prévues. Les points 1° et 3° de l'article 39 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[11] répriment d'une peine d'amende de 100€ à 100.000€ le traitement de données à caractère personnel en infraction aux conditions générales de licéité des traitements de données à caractère personnel énoncées à l'article 4 de la loi du 8 décembre 1992 (parmi lesquelles les principes de la collecte des données pour des finalités déterminées, explicites et légitimes et l'exclusion d'un traitement ultérieur de manière incompatible avec ces finalités) (art. 39, 1°) ainsi que le traitement de données à caractère personnel en violation des articles 6, 7 ou 8 de la loi du 8 décembre 1992 qui portent sur les données dites sensibles[12], les données relatives à la santé et les données judiciaires (art. 39, 2°). En cas de communication des données obtenues illégitimement à des tiers, l'article 458 du Code pénal, relatif à la violation du secret professionnel, peut également trouver à s'appliquer. Cette disposition prévoit une peine d'emprisonnement de 8 jours à 6 mois et une amende de 100€ à 500€. L'article 550bis, §1er, du Code pénal punit d'une peine d'emprisonnement de 3 mois à 1 an et/ou d'une peine d'amende de 26€ à 25.000€ « celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient », avec un alourdissement de la peine d'emprisonnement de 6 mois à 2 ans lorsque l'infraction est commise avec une intention frauduleuse. L'article 151 du Code pénal réprime, quant à lui, d'une peine d'emprisonnement de 15 jours à 1 an les actes arbitraires et attentatoires aux libertés et aux droits garantis par la Constitution ordonnés ou exécutés par un fonctionnaire ou officier public, ou par un dépositaire ou agent de l'autorité ou de la force publique.

12. La circulaire ministérielle GPI 75[13] rappelle que toute consultation par un membre du personnel des services de police ne peut avoir lieu que si elle est justifiée par un besoin opérationnel (c'est-à-dire qu'elle entre dans ses missions de police administrative ou judicaire) et que la consultation à des fins personnelles de la Banque de données Nationale Générale (ci-après dénommée BNG) est, notamment, constitutive d'une infraction à la loi sur la protection

---

[8] Règlement 2016/679 du Parlement et du Conseil 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.

[9] Directive commune MFO-3 du 14 juin 2002 des ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative.

[10] Arrêté royal du 10 mai 2006 fixant le Code de déontologie des services de police (*M.B.* du 30 mai 2006).

[11] (*M.B.* du 18 mars 1993).

[12] A savoir, les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle.

[13] Circulaire ministérielle GPI 75 du 15 octobre 2013 - Directive commune des ministres de la Justice et de l'Intérieur relative aux règles de procédure à suivre par les services de police dans le cadre de l'accès indirect aux données à caractère personnel qu'ils traitent dans la banque de données nationale générale dans le cadre de l'exercice de leurs missions de police judicaire et de police administrative.

de la vie privée passible de sanctions pénales. Cette circulaire ministérielle prévoit également la désignation au sein des services de la police intégrée de personnes de contact avec la Commission de la protection de la vie privée (ci-après dénommée CPVP).

13. L'article 9 de la loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle[14] a inséré un article 44/3 dans la loi sur la fonction de police, dont le 1er§ prévoit la création de la fonction de conseiller en sécurité et en protection de la vie privée au sein des services de police. Celui-ci a, entre autres, pour mission l'établissement, la mise en œuvre, la mise à jour et le contrôle d'une politique de sécurisation et de protection de la vie privée. Un arrêté royal peut fixer les règles selon lesquelles le conseiller en sécurité et en protection de la vie privée exerce ses missions.
Le nouvel article 44/3, §2 LFP prévoit par ailleurs la création d'une plate-forme de la sécurité et de la protection des données chargée de veiller à la réalisation coordonnée du travail des conseillers en sécurité et en protection de la vie privée. La composition et les modalités de fonctionnement de cette plate-forme ont été fixées par l'arrêté royal du 6 décembre 2015 relatif aux conseillers en sécurité et en protection de la vie privée et à la plate-forme de la sécurité et de la protection des données. Celui-ci est entré en vigueur le 1er mars 2016.

2.1.2. Banques de données accessibles

14. La principale banque de données policière est la BNG. Il s'agit d'une banque de données relationnelle policière dans laquelle des entités (personnes, organisations, moyens de transport, lieux, objets et numéros) sont enregistrées pour autant qu'elles puissent être au moins reliées à un fait prévu ou une enquête judicaire et que les conditions pour l'enregistrement soient remplies.

15. Dans le cadre de l'exercice de leurs missions de police administrative et judiciaire, les membres des services de police ont également accès à diverses banques de données. Les plus importantes sont le RRN (Rijksregister / Registre National), le RCA (Registre Central des Armes), le SIDIS (Système d'information des détentions / Detentie informatiesysteem) et la DIV (Banque de données de l'immatriculation des véhicules).

2.1.3. Accès aux banques de données en pratique

16. Les situations dans lesquelles les membres des services de police sont amenés à procéder à des interrogations des banques de données sont très nombreuses. Il est donc impossible de déterminer exhaustivement *a priori* toutes les situations dans lesquelles ces interrogations peuvent être légitimement effectuées (contrôles d'identité, enquêtes, missions de circulation, etc.). C'est, en fait, le contexte particulier et le cadre normatif spécifique qui déterminent si le membre du service de police peut procéder légitimement à l'interrogation de telle ou telle banque de données.

17. L'interrogation des banques de données peut se faire directement par le membre du service de police qui a l'autorisation d'y accéder en utilisant le portail informatique policier qui propose diverses applications permettant la consultation mais aussi, le cas échéant, en utilisant

[14] (*M.B.* du 15 octobre 2013).

des terminaux mobiles. La consultation peut également se faire par l'intermédiaire d'un tiers, notamment lorsque le membre du service de police n'a pas la possibilité d'y procéder lui-même (par exemple, un policier qui procède au contrôle d'une personne sur le terrain) ou par l'intermédiaire de terminaux spécifiques dans le cadre de fonctions spécialisées au sein de la police. Lors de l'interrogation de la banque de données « contrôle » de la BNG, la présence physique de l'entité contrôlée ou sa localisation physique suffisante dans l'espace est obligatoire pour permettre l'exécution des éventuelles mesures à prendre. La banque de données « contrôle » est mise à jour en temps réel et permet aux membres des services de police de s'assurer qu'une entité (personne, moyen de transport, numéro, objet) n'est pas signalée avec une mesure à prendre (arrestation, contrôle approfondi, etc.).

18. Les accès aux principales banques de données sont enregistrés (données d'identification du membre du personnel, poste de travail, données sur lesquelles l'interrogation de la banque de données ont porté, résultat de l'interrogation et motif de consultation enregistré). De même, les consultations (par exemple, la lecture ou l'impression d'un procès-verbal) au moyen de l'ISLP ('*Information System for Local Police*') ou de FEEDIS ('*Feeding Information System*' de la police fédérale) sont également enregistrées.

2.2. Mesures en vue de prévenir les abus

2.2.1. Note permanente de la police fédérale

19. En 2007, une note permanente[15] du commissaire général de la police fédérale, élaborée par la direction de l'information policière opérationnelle, a été adressée à tous les services de la police intégrée. Celle-ci aborde le prescrit légal, les principes en matière de traitement de l'information opérationnelle, les responsabilités et obligations des utilisateurs, diverses mesures préventives et enfin, le contrôle et le traitement des transgressions. En accord avec la CPPL, les chefs de corps de la police locale ont été invités à appliquer les mêmes mesures préventives à leur niveau. Cette note permanente du commissaire général de la police fédérale avait été diffusée, à l'époque, dans l'attente de l'approbation du livre 4 relatif à la protection de la vie privée de la directive ministérielle MFO-3. Ce livre 4 était sensé intégrer les directives énoncées dans la note permanente mais n'a finalement jamais vu le jour.

2.2.2. Information et sensibilisation du personnel

20. Dès 2004, un bulletin d'information[16] rappelait aux membres du personnel l'interdiction de consulter des banques de données à des fins privées. Suite à la diffusion de la note permanente du commissaire général du 9 octobre 2007, plusieurs documents internes ont traité de sujets en relation avec la problématique. De manière non exhaustive, on peut citer :

1) le bulletin « Info Nouvelles » N° 1808 du 18 octobre 2007 relatif au plan d'action contre l'utilisation irrégulière des informations qui, notamment, décrit ce qu'est une consultation illégitime et traite de la procédure de contrôle mise en place au sein de la police intégrée en incitant à remplir le motif de consultation. Le bulletin « Infodoc » N° 140

[15] Note permanente CGO-2007/3141 du 09/10/2007 du commissaire général de la police fédérale relative à la consultation des banques de données policières ou mises à disposition des services de police.

[16] Police fédérale, Direction des Relations internes, Bulletin d'information « Info-Nouvelles » N°1541, *Utilisation de l'information à des fins privées*, 12/05/2004.

d'octobre-novembre 2007 traite également du plan d'action spécifique envers l'utilisation irrégulière des informations ;

2) la note permanente DGS/DSJ-2008/4535/AJO du 31 janvier 2008 du commissaire général de la police fédérale adressée à toutes les entités de la police intégrée qui rappelle que les données à caractère personnel en possession des services de police ne peuvent être transmises qu'aux destinataires prévus par l'article 44/1, alinéas 3 et 5 de la LFP ;

3) le bulletin d'information « CGO News » du 7 juillet 2011 qui constitue un rappel en matière de consultation des banques de données policières ;

4) la note temporaire CGO-2011/5273 du 25 octobre 2011 du directeur CGO adressée à toutes les entités de la police intégrée relative aux modalités d'accès aux photos disponibles par consultation du RRN ;

5) le bulletin d'information « CGO News » du 12 mai 2014 relatif à la consultation des banques de données qui reprend de manière détaillée les règles fondamentales pour la consultation des bases de données accessibles aux services de police ;

6) les bulletins d'information « DRI News » N° 112 du 24 juin 2016 et « Info Nouvelles » N° 2405 du 24 juin 2016 relatifs aux adaptations techniques mises en œuvre dans le cadre du SSO (*'Single Sign On'*) suite aux recommandations émises en 2015 dans le cadre de l'évaluation du groupe de travail SCHEVAL[17]. Il s'agit d'un développement technique harmonisant les « *logins* » et empêchant qu'un utilisateur « Windows » soit différent d'un utilisateur « Portal »[18] sur une station de travail ;

7) le bulletin « Info Nouvelles » N° 2407 du 8 juillet 2016, « *Banques de données, intégrité et vie privée* », reprend la nouvelle approche de la DRI et son plan d'action ;

8) le bulletin « DRI News » N° 114 du 18 août 2016 relatif aux mots de passe vise notamment à l'utilisation de mots de passe respectant des standards minima[19].

21. Dans le prolongement de la note permanente du commissaire général du 9 octobre 2007 et du plan d'action visant à lutter contre les abus, un espace spécifique, dédié aux consultations irrégulières des données, a été créé sur l'intranet policier. Cet espace est géré par la DRI. Par ce canal, les membres de services de police ont accès aux diverses publications (notes, feuillets d'information, etc.) ainsi qu'à un rappel de la législation en la matière. Un quizz destiné à tester les connaissances du personnel est également disponible. Une diminution de la fréquentation de ce site[20] peut être constatée pour la période 2009-2014. Il convient cependant de considérer, à cet égard, que le site fournit essentiellement un appui « documentaire » et que la plupart des documents sont disponibles au sein des services de police. De plus, la police ayant entrepris

[17] Le groupe de travail SCHEVAL ('Schengen Evaluation Working Group') a notamment pour tâche d'évaluer la manière dont les signataires du traité de Schengen respectent les règles et si les États membres sont suffisamment préparés pour les mettre en œuvre. Plusieurs plans d'action sont développés à la police fédérale afin de répondre à des recommandations formulées.

[18] Portail informatique sur l'intranet policier disponible sur certaines stations de travail donnant notamment accès aux banques de données accessibles aux membres des services de police.

[19] Une note permanente CG-ISPO-20165/1858 du 29/04/2016 relative à la sécurité des informations a été élaborée par la police fédérale. Elle fixe notamment un standard minimum pour la création et l'utilisation des mots de passe qui doivent être implémentés au sein des systèmes informatiques gérés ou qu'elle met à disposition des utilisateurs. Cette note est d'application pour l'ensemble des utilisateurs de ces systèmes.

[20] Nombre moyen mensuel de visites du site : 437,5 visites en 2009, 738,4 en 2010, 549,8 en 2011, 359,8 en 2012, 274,4 en 2013 et 197,9 en 2014.

d'aborder sérieusement la problématique des consultations irrégulières dès 2007 / 2008, l'intérêt spécifique du début s'est vraisemblablement un peu émoussé avec le temps.

22. Un avis rappelle également de manière systématique aux membres des services de police qui accèdent au portail informatique policier en vue d'interroger les banques de données que les consultations sont enregistrées, susceptibles d'être contrôlées et que l'information ne peut être traitée que dans le cadre de missions de police administrative et/ou judiciaire.

23. Ces différentes mesures d'information et de sensibilisation du personnel permettent d'affirmer que les membres de la police intégrée paraissent suffisamment informés des contraintes et restrictions liées à la consultation des banques de données mises à leur disposition. C'est d'ailleurs la raison pour laquelle la DRI souhaite passer de la simple sensibilisation à la conscientisation des membres des services de police.

2.2.3. Gestion des autorisations d'accès

24. C'est la DRI qui exerce la gestion, le contrôle et l'appui en ce qui concerne l'attribution des accès aux banques de données d'appui et à la BNG[21]. Il appartient aux responsables policiers de personnaliser les accès de manière à ce qu'ils soient en concordance avec les tâches exercées par les membres du personnel concernés. Le principe est donc de n'attribuer aux membres du personnel que l'accès aux applications dont ils ont la réelle utilité[22]. Il arrive parfois que les demandes d'accès présentant un caractère interpellant soient réévaluées avec le demandeur (par exemple, des demandes d'accès pour l'ensemble d'un service ou des demandes d'accès aux banques de données opérationnelles pour des membres du personnel occupant des fonctions purement administratives). La DRI traite en moyenne journalièrement dix courriels ayant trait à des demandes d'accès pour des membres du personnel de la police intégrée. Lorsqu'un membre des services de police se trouve en non-activité suite à sa pension ou en raison d'un congé de longue durée, son statut est modifié dans la banque de données de gestion du personnel ce qui génère automatiquement le retrait de ses autorisations d'accès aux banques de données. Dans le cadre de ses fonctions, la DRI peut également adresser des « signaux » aux responsables policiers sur la base des constatations tirées, entre autres, du programme de gestion des accès (par exemple, un accès qui n'a pas été utilisé durant une longue période pourrait remettre en question le réel besoin d'en connaître de l'utilisateur concerné). Il est prévu de développer cette approche avec la CPPL dans le cadre des actions à venir.

25. Le profil « standard » qui permet aux membres des services de police d'accomplir les tâches de base qui lui sont confiées (accueil/intervention/'*community policing*', …) comprend généralement (mais pas obligatoirement) l'accès aux applications « Contrôle », « Consultation faits concrets », « DIV non urgent », « RPO » (Recherches sur numéros de marque d'immatriculation incomplets), « RRN », « RCA », « SIDIS » et « mailing ». L'accès à d'autres applications plus spécifiques comme la consultation des faits non-concrets, des enquêtes ou de la photothèque est réservé aux membres du personnel ayant des fonctions plus spécifiques, comme les membres des services judicaires ou des SICAD (Service d'information et de communication d'arrondissement). Fin mai 2015, 84,60% des membres des services de police (membres opérationnels et CALOG) avaient accès à l'application « consultation » de la BNG. 81,20% avaient accès à l'application « contrôle ». 89% des membres de la police intégrée avaient accès au RRN fin juillet 2015. Le nombre relativement important de membres du personnel ayant accès au RRN s'explique par le fait que cette banque de données est

[21] La DRI s'occupe également des accès aux faits non concrets en ce qui concerne la police locale.
[22] Les accès aux banques de données sont personnalisables, banque de données par banque de données.

indispensable dans l'exécution des missions de police tant pour les membres du cadre opérationnel (rédaction des procès-verbaux, perquisitions, interventions, signalements, contrôles d'identité, ...) que pour certains membres CALog qui effectuent des tâches en appui de leurs collègues opérationnels (accueil, enregistrement dans les banques de données, etc.). Les différences constatées en ce qui concerne le nombre d'accès octroyés pour les différentes applications est logique. Elles démontrent qu'une distinction est faite entre les membres du personnel lors de l'octroi des accès.

2.2.4. Motif de consultation

26. La note permanente du commissaire général de la police fédérale du 9 octobre 2007 recommande d'indiquer le motif de consultation des banques de données lorsqu'il est possible de pratiquer de la sorte et, spécifiquement, lorsque la consultation a été effectuée au profit d'un autre membre des services de police. Comme le précise ce document, cette pratique n'est pas toujours possible en toutes circonstances. On peut penser, à cet égard, aux membres du personnel qui consultent intensivement les banques de données (personnel des SICAD, gestionnaires fonctionnels dans les zones de police, personnel dans les dispatchings locaux, etc.) pour lesquels il serait pratiquement impossible de satisfaire à une obligation d'indiquer un motif de consultation.

27. Pratiquement, le membre du service de police qui consulte une banque de données a la possibilité d'enregistrer le motif de consultation dans un champ prévu à cet effet. En ce qui concerne la consultation des photos du RRN, l'indication d'un motif de consultation est obligatoire. Celui-ci doit être suffisamment clair pour permettre d'établir facilement la légitimité de la consultation. Un récent feuillet d'information[23] encourage une fois de plus vivement l'utilisation du champ « motif de consultation » qui est d'ailleurs considéré comme un véritable aide-mémoire puisque le contenu de ce champ est enregistré dans les « *loggings* », au même titre que les autres traitements effectués dans l'application concernée.

2.2.5. « Logging » des utilisations et contrôles a posteriori des accès

28. Chaque utilisation des applications de la BNG, du RRN et de la DIV est enregistrée dans un « *logging* » disponible pendant cinq ans. En vertu de la directive ministérielle MFO-3, les données de « *logging* » peuvent être utilisées à des fins de contrôle de la légalité de l'utilisation des banques de données, à des fins de contrôle préventif des consultations et contrôles effectués par les membres des services de police et à des fins opérationnelles pour, notamment, vérifier si une personne ou un moyen de transport a été contrôlé par un service de police.

29. En accord avec la CPPL, la DRI transmet, chaque mois, des « *loggings* » de consultations aux responsables policiers (chefs de corps de la police locale ou directeurs de services de la police fédérale) d'une zone de police francophone, d'une zone de police néerlandophone et d'un service de la police fédérale. Une dizaine de membres représentatifs du personnel est sélectionnée de manière aléatoire au sein de chaque service de police concerné par le contrôle (membres du corps opérationnel ou administratif, consultants externes, membres de services centraux ou d'antennes, etc.). Les données des « *loggings* » portent sur des périodes de plusieurs jours (semaine et week-end) du mois précédant l'extraction des données. De manière plus irrégulière, des contrôles sont effectués par la DRI sur base de l'actualité médiatique (par

[23] Police fédérale, CGO, CGO News N°43, *Consultation des bases de données*, 12/05/2014.

exemple, lors de l'élection de Miss Belgique en vue de détecter d'éventuelles consultations des données du RRN par curiosité). À chaque fois, l'attention des responsables policiers est attirée sur le cadre légal relatif aux consultations des banques de données, sur l'existence d'un site spécialement dédié à cette problématique sur le portail informatique policier ainsi que sur la nécessité de prendre les mesures nécessaires en cas d'irrégularité constatée. Il appartient aux responsables policiers locaux et fédéraux de procéder aux vérifications nécessaires afin d'établir la légitimité des consultations effectuées par les membres de leur personnel. La DRI souligne que le premier objectif des contrôles n'est pas le traitement des « *loggings* » en soi mais plutôt la sensibilisation, de manière personnalisée et concrète, des responsables des services de police quant à la problématique des consultations irrégulières et, partant, de les inciter à prendre les mesures nécessaires à leur niveau de manière proactive. DRI est conscient que le contrôle organisé de la sorte n'est pas significatif eu égard au nombre de contrôles effectués journalièrement dans les banques de données au sein de la police intégrée. Néanmoins, celui-ci doit, en principe, permettre de déboucher *in fine* sur un nombre plus significatif de contrôles. Les contrôles étant effectués dans le respect de l'autonomie des zones de police locale, aucun feed-back n'est exigé.

30. Trois zones de police locale ayant reçu récemment pareils « *loggings* » ont été interrogées fin 2015 afin d'obtenir des informations quant à la manière dont elles ont concrètement abordé ces contrôles. Deux zones de police sur les trois ont exploité le « *logging* » qui leur avait été transmis. La troisième zone n'a pas du tout exploité le document en raison de la charge de travail que cela représente. Une zone de police a transmis à chaque membre du personnel concerné le listing des consultations sélectionnées en lui demandant de préciser par écrit, pour chacune d'entre elles, les références des documents permettant de les justifier (par exemple, un numéro de procès-verbal ou de fiche d'information). Sur base des informations fournies, des vérifications complémentaires ont été effectuées par le responsable du contrôle afin de vérifier la légitimité de la consultation. Lorsqu'un contrôle n'a pu être justifié par l'existence d'un document, le membre du personnel en a fait état dans son rapport sans que ces consultations ne soient, pour autant, considérées comme illégitimes ou problématiques. Dans l'autre zone de police, le contrôle a consisté en l'établissement d'une relation entre les consultations effectuées et un document enregistré sur base du service des collaborateurs concernés. Aucune information complémentaire n'a été demandée au personnel.

31. Les informations recueillies lors de la consultation des trois zones de police sont très parcellaires et ne peuvent être extrapolées à l'ensemble des services de police. Elles permettent cependant de tirer quelques enseignements. Le but premier poursuivi par les contrôles *a posteriori* est la sensibilisation des responsables policiers à la problématique. Si cet objectif peut être effectivement atteint de cette manière, c'est cependant le contrôle de la légitimité des consultations qui constitue, apparemment, la première préoccupation des responsables policiers chargés de procéder concrètement au contrôle. Ils effectuent celui-ci en fonction de leur propre perception en tenant notamment compte de la charge de travail qu'il implique. La vérification minutieuse de la légitimité des consultations requiert, en effet, une charge de travail qui n'est pas à négliger. Un chef de corps consulté a, d'ailleurs, suggéré que des contrôles approfondis soient limités aux consultations pour lesquelles il existerait des « signaux » révélant une éventuelle situation problématique afin de limiter la charge de travail. Même s'il a le mérite d'exister et poursuit un objectif louable, il paraît utile de s'interroger sur l'opportunité de maintenir un système de contrôle reposant sur la vérification de la légitimité de consultations sélectionnées de manière aléatoire en dehors de tout élément de suspicion concret de dysfonctionnement. En outre, compte tenu de la rareté des contrôles, la sensibilisation espérée des responsables policiers a vraisemblablement un effet de rémanence limité.

32. Le système de contrôle devrait évoluer prochainement. DRI prévoit de cesser de procéder aux contrôles *a posteriori* dans leur forme actuelle, tous les services de police ayant été soumis une fois à la procédure de contrôle instaurée dans le prolongement de la note permanente du commissaire général de la police fédérale de 2007.

2.2.6. Projet de directive régissant l'accès, l'utilisation et le contrôle des moyens ICT au sein de la police fédérale

33. Une directive régissant l'accès, l'utilisation et le contrôle des moyens ICT au sein de la police fédérale est en cours de finalisation. Celle-ci s'applique également à l'utilisation des moyens ICT qui permettent tout traitement de données à caractère personnel sensibles et, plus particulièrement, les informations et les données à caractère personnel enregistrées dans les banques de données visées à l'article 44/2 de la LFP et les données relatives à la santé. Compte tenu de la sensibilité de ces données, il est prévu que des règles spécifiques soient édictées.

34. La police fédérale est, apparemment, la seule administration publique qui ait élaboré une directive qui s'applique à un nombre aussi diversifié de moyens ICT. Celle-ci entend concilier le respect du droit fondamental des utilisateurs au respect de leur vie privée dans la relation de travail et les nécessités d'un bon fonctionnement de la police fédérale. Elle énumère de manière précise les activités interdites et décrit aussi les modalités générales d'exercice du contrôle qui repose sur quatre principes : principe de finalité, principe de proportionnalité, principe de subsidiarité et principe de transparence.

35. Le contrôle prévu doit reposer sur au moins une des finalités suivantes :

1) la constatation d'infractions pénales notamment diffamatoires, de faits contraires aux bonnes mœurs ;
2) la protection des informations qui concernent le fonctionnement opérationnel de la police et celles auxquelles est rattaché un degré de protection ;
3) la sécurité et/ou le bon fonctionnement technique des systèmes informatiques de la police en général ;
4) le respect de la directive et des règles d'utilisation des moyens ICT en vigueur au sein de la police fédérale ainsi que du code de déontologie.

36. Le contrôle doit également être effectué dans le respect des principes de proportionnalité et de subsidiarité, ce qui implique que la collecte des données à caractère personnel est limitée à ce qui est strictement nécessaire dans le cadre des finalités du contrôle, que les données collectées doivent être adéquates, pertinentes et non excessives au regard de ces finalités et que les contrôles ciblés doivent être ponctuels et justifiés par des indices laissant suspecter une anomalie ou une utilisation abusive des moyens ICT.

37. En vertu du principe de transparence, les membres de la police fédérale doivent être informés au niveau collectif et individuel de la politique de contrôle à leur égard, du type de contrôle et de la manière dont il est effectué.

38. Le contrôle comprend deux étapes : un contrôle général et un contrôle ciblé et individualisé. Les contrôles ciblés sont ponctuels et justifiés par des indices laissant suspecter une anomalie ou une utilisation abusive des moyens ICT.

39. Le projet de directive a été soumis à la CPVP pour avis informel et les apports de cette institution ont été intégrés dans le texte. Il a été soumis à la concertation syndicale en juillet 2016 et devrait entrer en vigueur début 2017 après, notamment, l'élaboration d'un plan de communication.

2.2.7. Plan d'action dans le cadre de la bonne utilisation des banques de données de la police ou de celles mises à sa disposition

40. Un nouveau plan d'action dont les grandes lignes s'articulent autour de la consultation mais aussi de l'accès aux banques de données a été récemment mis en place par la DRI. Les axes principaux de ce plan d'action sont le suivants :

1) le suivi et la gestion des accès et des consultations ;
2) le contrôle préventif ciblé des consultations ;
3) l'élargissement du champ d'application aux banques de données non opérationnelles ;
4) l'appui de la DRI dans les initiatives prises au niveau local pour l'élaboration d'un plan d'action en la matière ;
5) la communication qui se veut non seulement toujours transparente mais aussi plus diversifiée en reprenant également les actions menées par la DRI et les résultats obtenus.

2.3. Dysfonctionnements

2.3.1. Analyse complémentaire

41. Complémentairement à l'analyse détaillée des plaintes et dénonciations 2013 communiquées au Comité P en matière d'atteinte à la vie privée effectuée dans le cadre du rapport annuel 2013, une analyse des données dépersonnalisées de la banque de données « jurisprudence » du Conseil de discipline a été effectuée pour la période 2012-2015. Celle-ci permet d'obtenir des informations pertinentes concernant des dysfonctionnements avérés. Les qualifications dépersonnalisées des infractions disciplinaires fournissent cependant peu de données de contexte.

42. La base de comptage utilisée lors de cette analyse est la sanction disciplinaire infligée à un membre de la police intégrée. Elle est donc différente de celle utilisée lors de l'analyse des données du Comité P (allégations d'accès illégitimes lors des plaintes et dénonciations en 2013). Il n'est donc pas possible de comparer directement les chiffres des deux analyses.

2.3.2. Ampleur de la répression disciplinaire

Tableau 3 : Sanctions disciplinaires infligées (nombre de sanctions disciplinaires)

Sanctions disciplinaires	2012	2013	2014	2015	Période 2012-2015
	48	59	63	40	210

Source : Banque de données « jurisprudence » du Conseil de discipline

43. Une diminution de 16,66% du nombre de sanctions disciplinaires est constatée sur la période 2012-2015. La tendance générale est négative ce qui tend à démontrer que le phénomène se résorbe ou que la répression en la matière est moins efficace ou intensive. Cette diminution importante en pourcentage doit cependant être relativisée compte tenu des chiffres peu élevés dont il est question. De plus, il existe vraisemblablement un chiffre noir en raison de la difficulté de détecter les dysfonctionnements (voir infra). Les sanctions disciplinaires infligées en 2015 concernent environ 0,08% des membres de la police intégrée[24].

Tableau 4 : Suites « disciplinaires » signalées au Comité P[25] (nombre d'allégations d'accès illégitimes établies)

Suites « disciplinaires »	2013	%
Rappels à la norme (Remarques, notes de fonctionnement, etc.)	15	23,44%
Sanctions disciplinaires légères	13	20,31%
Sanctions disciplinaires lourdes	6	9,38%
Classement sans suite mais transaction pénale	4	6,25%
Dossier disciplinaire avec décision inconnue	1	1,56%
Suspension provisoire avec retenue de traitement	1	1,56%
Informations insuffisantes	24	37,50%
Total	64	100,00%

Source : Base de données du Comité P

44. En 2013, sur les 64 allégations d'accès illégitimes établies, ce sont essentiellement des mesures de rappel à la norme (23,44%) et des sanctions disciplinaires légères (20,31%) qui ont été prises. Il convient de noter que 12 autres dossiers disciplinaires étaient toujours pendants (allégations d'accès illégitimes non forcément établies) lors du signalement des faits au Comité P. La différence entre les chiffres de la banque de données « jurisprudence » du Conseil de discipline et ceux de la base de données du Comité P est vraisemblablement due, en partie, au fait que l'examen de la pertinence des allégations d'accès illégitimes n'était pas terminé lors du signalement des faits au Comité P.

[24] Sur la base des 49 218 membres de la police intégrée recensés en mai 2015.

[25] En application de l'article 14bis, alinéa 2, de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace.

2.3.3. Contexte des accès illégitimes

Tableau 5 : Contexte des accès illégitimes sanctionnés (nombre de sanctions disciplinaires)

Contexte	2012	2013	2014	2015	Période 2012-2015	%
En dehors du cadre professionnel	46	57	60	33	196	93,33%
Dans le cadre professionnel	1	1	1	0	3	1,43%
Indéterminé	1	1	2	7	11	5,24%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

45. Ce sont principalement des consultations des banques de données en dehors du cadre professionnel qui constituent l'essentiel des accès illégitimes sanctionnés (93,33%). 77,78% des allégations d'accès illégitimes répertoriées dans la base de données du Comité P en 2013 s'inscrivaient également en dehors du cadre professionnel (9,52% dans le cadre professionnel et 12,70% dans un contexte indéterminé). Ces consultations sont principalement motivées par des considérations d'ordre privé.

46. Nonobstant le peu d'informations disponibles relatives au contexte des faits sanctionnés, on peut cependant relever que dans quatre cas, la consultation des banques de données s'est faite en utilisant l'accès informatique d'un autre policier. Dans deux cas, la consultation a été demandée à un collègue. Dans un cas, un motif de consultation fallacieux a été utilisé.

2.3.4. Récurrence des accès illégitimes

Tableau 6 : Récurrence des accès illégitimes sanctionnés (nombre de sanctions disciplinaires)

Récurrence	2012	2013	2014	2015	Période 2012-2015	%
Accès illégitime unique	17	21	16	10	64	30,48%
Plusieurs accès illégitimes	20	21	16	8	65	30,95%
Nombreux accès illégitimes	1	4	6	7	18	8,57%
Indéterminé	10	13	25	15	63	30,00%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

Tableau 7 : Récidive des membres des services de police sanctionnés (nombre de sanctions disciplinaires)

Récidive	2012	2013	2014	2015	Période 2012-2015	%
Récidive	0	0	3	0	3	1,43%
Pas de récidive	48	59	60	40	207	98,57%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

47. Le nombre de dossiers dans le cadre desquels de nombreux accès illégitimes ont été constatés est, heureusement, assez faible (8,57% des sanctions disciplinaires et 10,32% des allégations en 2013 dans la base de données du Comité P). On peut cependant regretter que le pourcentage de cas où il est question de plusieurs accès illégitimes soit si élevé (30,95% des sanctions disciplinaires et 23,02% des allégations en 2013 dans la base de données du Comité P). Le taux de récidive est apparemment très faible.

2.3.5. Membres du personnel en cause

Tableau 8 : Cadre auquel les membres des services de police sanctionnés appartiennent (nombre de sanctions disciplinaires)

Cadre	2012	2013	2014	2015	Période 2012-2015	%
CALOG	4	5	10	1	20	9,52%
Agent de police	7	6	4	2	19	9,05%
Cadre de base	26	34	36	31	127	60,48%
Cadre moyen	7	11	10	5	33	15,71%
Cadre officier	4	3	2	1	10	4,76%
Aspirant inspecteur	0	0	1	0	1	0,48%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

Tableau 9 : Composante de la police intégrée à laquelle les membres des services de police sanctionnés appartiennent (nombre de sanctions disciplinaires)

Composante de la police intégrée	2012	2013	2014	2015	Période 2012-2015	%
Police locale	41	47	51	32	171	81,43%
Police fédérale	7	12	12	8	39	18,57%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

Tableau 10 : Rôle linguistique des membres des services de police sanctionnés (nombre de sanctions disciplinaires)

Rôle linguistique	2012	2013	2014	2015	Période 2012-2015	%
Francophone	24	29	33	25	111	52,86%
Néerlandophone	24	30	29	15	98	46,66%
Germanophone	0	0	1	0	1	0,48%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

48. Le profil type du membre du service de police accédant illégitimement à une base de données semble donc être celui d'un membre de la police locale appartenant au cadre opérationnel de base. Il semble y avoir (proportionnellement à l'effectif) plus de membres des services de police francophones, à moins que la détection de cas d'abus soit plus active dans la partie francophone.

2.3.6. Banques de données consultées et utilisation des données

Tableau 11 : Banques de données consultées par les membres des services de police sanctionnés (nombre de sanctions disciplinaires) [26]

Banque de données consultées	2012	2013	2014	2015	Période 2012-2015	%
RRN	19	31	13	4	67	31,90%
BNG	12	14	2	2	30	14,28%
DIV	7	4	5	4	20	9,52%
ISLP/FEEDIS	4	5	5	1	15	7,14%
Insuffisamment précisée(s)	16	18	44	31	109	51,90%

Source : Banque de données « jurisprudence » du Conseil de discipline

49. Ces chiffres sont à comparer aux allégations d'accès illégitimes enregistrées en 2013 dans la base de données du Comité P : RRN (40,48% des allégations d'accès illégitimes), DIV (11,11%), BNG (8,73%) et ISLP (4,76%). Les accès au registre national constituent donc assez invariablement la majeure partie des accès illégitimes. Les sanctions disciplinaires pour accès illégitimes au RRN semblent diminuer fortement en 2014 et surtout en 2015. Il est cependant possible que pas mal d'accès illégitimes au RRN n'aient pas été clairement mentionnés ces deux dernières années dans le libellé des infractions disciplinaires sanctionnées.

50. Les consultations des données du RRN paraissent constituer les atteintes les plus sérieuses à la protection de la vie privée du citoyen. Il convient toutefois de considérer que les consultations illégitimes d'autres données à la disposition des membres de services de police sont souvent ressenties par les victimes comme des atteintes à la « *privacy* » plus sérieuses (information sur les détentions subies ou les faits commis, par exemple).

[26] Plusieurs banques de données peuvent avoir été consultées dans le cadre d'une même sanction disciplinaire. Le pourcentage est calculé par rapport au nombre de sanctions disciplinaires pour la période 2012-2015.

Tableau 12 : Utilisation de l'information acquise illégitimement par les membres des services de police sanctionnés (nombre de sanctions disciplinaires)

Utilisation de l'information acquise	2012	2013	2014	2015	Période 2012-2015	%
Diffusion d'informations à des tiers	13	10	6	4	33	15,71%
Évocation de l'information	0	3	0	0	3	1,43%
Utilisation active (contacter, etc.)	1	0	1	0	2	0,95%
Indéterminé(e)	34	46	56	36	172	81,91%
Total	48	59	63	40	210	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

51. Les motifs des sanctions disciplinaires n'abordent pas explicitement l'utilisation de l'information dans 81,91% des cas. Les utilisations de l'information connues précisément concernent principalement des diffusions de l'information à des tiers ou des évocations de celle-ci.

2.3.7. Nature des sanctions disciplinaires

Tableau 13 : Nature des sanctions disciplinaires (nombre de sanctions disciplinaires)

Nature des sanctions disciplinaires	2012	2013	2014	2015	Période 2012-2015	%	Période 2001-2015	%
Avertissement	13	17	17	9	56	26,66%	141	27,65%
Blâme	17	25	24	12	78	37,14%	201	39,41%
Retenue de traitement	7	8	15	13	43	20,48%	89	17,45%
Suspension	6	8	7	1	22	10,48%	43	8,43%
Rétrogradation	1	0	0	0	1	0,48%	15	2,94%
Démission d'office	4	1	0	5	10	4,76%	21	4,12%
Total	48	59	63	40	210	100,00%	510	100,00%

Source : Banque de données « jurisprudence » du Conseil de discipline

52. Dans la majorité des cas, ce sont des sanctions disciplinaires légères qui sont appliquées, apparemment, en raison du fait qu'il s'agit de consultations illégitimes sans utilisation spécifique de l'information. D'autres faits que les accès illégitimes aux banques de données peuvent être concernés par les sanctions infligées (diffusion volontaire de l'information à des tiers, évocation indue de l'information, etc.). Ceux-ci sont évidemment de nature à aggraver la sanction disciplinaire infligée. Les pourcentages pour la période 2012-2015 et pour la période 2001-2015 sont globalement assez similaires.

2.3.8. Dysfonctionnements organisationnels

53. Les sanctions disciplinaires sont appliquées, en règle générale, pour des dysfonctionnements individuels et non des dysfonctionnements organisationnels de sorte que

l'examen des données de la banque de données « jurisprudence » du Conseil de discipline n'est pas d'un grand secours. L'examen des allégations d'accès illégitimes enregistrées en 2013 dans la base de données du Comité P a seulement permis de détecter quelques dysfonctionnements organisationnels : dans le cadre d'un litige avec un collègue, obtention par un policier d'un « *logging* » relatif aux consultations le concernant en motivant sa demande par une finalité de contrôle interne, utilisation par un aspirant policier de l'accès de son mentor à des fins illégitimes et non-exécution d'un suivi proactif par une zone de police locale.

54. La détection d'éventuels dysfonctionnements organisationnels et structurels au sein des services de police demande des investigations spécifiques assez lourdes. Il n'est donc pas possible de conclure au stade actuel sur ce point. La création de la fonction de conseiller en sécurité et en protection de la vie privée devrait permettre, à l'avenir, d'aborder les éventuels problèmes organisationnels qui se présentent sur ce plan dans les corps de police de manière structurée et obligatoire.

2.3.9. Répression pénale

Tableau 14 : Suites judiciaires encourues par les membres des services de police en cause (nombre d'allégations d'accès illégitimes)

Suites judiciaires	2013	%
Classement sans suite	20	22,73%
Transaction	14	15,91%
Citation correctionnelle	1	2,28%
Inconnues	52	59,09%
Total	88	100,00%

Source : Base de données du Comité P

Tableau 15 : Motifs de classement sans suite (nombre d'allégations d'accès illégitimes)

Motif de classement sans suite par les Parquets	2013	%
Pas d'infraction	2	10,00%
Preuves insuffisantes	2	10,00%
Charges insuffisantes	3	15,00%
Conséquences disproportionnées des poursuites pénales	2	10,00%
Renvoi vers la médiation pénale	1	5,00%
Fait occasionnel	1	5,00%
Inconnu	9	45,00%
Total	20	100,00%

Source : Base de données du Comité P

55. Les allégations traitées sur le plan judiciaire ont surtout donné lieu à des transactions pénales, un seul cas ayant abouti à des poursuites correctionnelles. Le plan du ministre de la Justice prévoit d'approcher de manière plus efficiente la criminalité. Compte tenu de cette tendance, il est peu vraisemblable qu'une aggravation de la répression en matière d'accès

illégitimes simples, sans utilisation spécifique des données consultées illicitement, puisse être envisagée. En tout état de cause, comme par le passé, le Comité P entend systématiquement dénoncer au parquet les accès illégitimes aux banques de données qu'il constate.

2.4. Difficulté d'établir les abus

56. Les accès illégitimes aux banques de données sont relativement faciles à établir en cas de plainte ou dénonciation lorsque des éléments précis permettent d'orienter les recherches et de les limiter. Il n'en est pas de même lorsque, par exemple, la consultation a été effectuée par l'intermédiaire de l'accès d'un autre membre du personnel, sans indication du motif de consultation, ou lorsque les investigations portent sur de possibles abus peu contextualisés.

57. L'établissement du caractère légitime des consultations peut être grandement facilité lorsque le motif de consultation est enregistré de manière suffisamment explicite pour le contrôleur et le membre du personnel qui doit se justifier. À l'occasion d'une enquête récente du Service d'enquêtes P, l'examen du motif des consultations de photos dans le RRN au sein d'une zone de police - qui doit obligatoirement être complété - a révélé que seulement 12,1%[27] des consultations étaient motivées par une référence suffisamment claire. Dans les autres cas, les motivations utilisées ne permettaient pas d'établir immédiatement et facilement le lien entre la consultation du RRN et le dossier qui a donné lieu à la consultation. De manière générale, il ressort fréquemment des enquêtes menées que les motifs de consultation enregistrés sont insuffisants pour pouvoir légitimer les consultations des banques de données.

58. Lorsqu'aucun motif de consultation n'est enregistré, lorsque le motif de consultation est insuffisamment précis ou lorsque le membre du service de police ne se souvient pas de la consultation et de son contexte, il est nécessaire d'effectuer des vérifications complémentaires fastidieuses afin d'établir le lien avec une mission de police judiciaire ou administrative. De nombreuses vérifications de ce type pour un nombre important de consultations sont impossibles à envisager en raison de la charge de travail que cela suppose.

2.5. Persistance des consultations illégitimes

59. La persistance des consultations illégitimes, malgré le dispositif préventif et répressif, peut s'expliquer par différents facteurs. Tout d'abord, force est de constater que la majorité des accès illégitimes sont révélés par le biais des plaintes et dénonciations, certains faits ayant attiré l'attention des victimes ou des dénonciateurs (par exemple l'évocation par l'auteur de l'accès illégitime d'éléments d'information qui ne sont disponibles que par la consultation d'une base de données spécifique). Un accès illégitime se limitant à la simple prise de connaissance de l'information, non accompagné de « publicité » ou d'action révélatrice du dysfonctionnement, sera difficilement détectable. C'est d'autant plus vrai que la probabilité pour un membre des services de police lambda de subir un contrôle portant sur un éventuel accès illégitime commis est fort réduite dans le cadre du dispositif de contrôle actuel. Un autre facteur explicatif réside dans une certaine « compréhension » pour des consultations, certes illégitimes, mais jugées « acceptables » en raison de la nature de la motivation sous-jacente (la préoccupation quant au nouvel environnement familial de ses enfants, par exemple) ou en raison de la gravité « relative » des consultations elles-mêmes (la consultation de ses propres données RRN ou la consultation de données par simple curiosité, par exemple). La proportion importante d'accès

[27] Sur une période de près de trois ans.

illégitimes ayant donné lieu à un simple rappel à la norme (23,44% des allégations d'accès illégitimes établies en 2013) illustre cette constatation. On se souviendra également que lors de l'analyse des plaintes et dénonciations portées à la connaissance du Comité P en 2013, il avait été constaté qu'un peu plus d'un tiers (35,79%) des allégations d'accès illégitimes avérés semblait avoir été traité exclusivement en interne sur le plan disciplinaire par les services de police sans que les faits n'aient été portés à la connaissance de l'autorité judiciaire.

2.6. Pistes de réflexion

2.6.1. Généralités

60. Différentes pistes peuvent être explorées afin d'envisager des solutions complémentaires ou alternatives au dispositif préventif et répressif existant. Les aménagements ne doivent cependant pas conduire à alourdir administrativement la tâche des membres des services de police ou être de nature à les amener à hésiter à consulter les banques de données, ce qui nuirait globalement à l'exécution du travail policier. Un équilibre doit être recherché entre la prévention des abus et l'efficacité policière opérationnelle.

61. La création de la fonction de conseiller en sécurité et en protection de la vie privée au sein des services de police, telle que prévue par l'article 44/3 LFP, constitue une opportunité évidente afin de conscientiser véritablement les responsables policiers à la problématique de l'accès illégitime aux banques de données et de dépasser le stade de la seule information et sensibilisation des membres des services de police.

2.6.2. Prévention des abus

- *Enregistrement du motif de consultation*

62. L'enregistrement du motif de consultation constitue un moyen dissuasif et préventif des abus. En effet, l'enregistrement d'un motif fallacieux peut, le cas échéant, constituer un faux informatique et un frein aux consultations illégitimes. Il peut cependant être contre-indiqué de l'imposer, par exemple, lorsque des données sensibles sont traitées par certains services de police ou lorsque l'imposition de cette pratique entraînerait une surcharge administrative trop importante en raison du volume de données à traiter (gestionnaires fonctionnels, par exemple).

63. Le seul enregistrement d'un motif ne constitue cependant pas, à lui seul, la preuve de la légitimité d'une consultation. Lors d'enquêtes sur des suspicions de consultations illégitimes, seules des vérifications plus fouillées permettent d'établir leur caractère légitime ou non. En effet, il ne peut jamais être exclu, même s'il s'agit de cas assez marginaux, qu'un motif de consultation fallacieux ait été enregistré. Le motif est donc, en réalité, un aide-mémoire pour le membre des services de police qui doit être à même de pouvoir justifier la légitimité de sa consultation. Il faut également insister sur le fait que l'établissement du caractère légitime de la consultation ne peut être grandement facilité que si le motif enregistré est suffisamment explicite tant pour le « contrôleur » que pour le membre du personnel qui est amené à devoir se justifier.

64. Comme on l'a vu, l'enregistrement du motif de consultation n'est obligatoire, à l'heure actuelle, que lors de la consultation des photos du RRN. Les différents documents policiers qui

abordent la thématique de la consultation des banques de données n'ont cependant eu de cesse, tout comme le Comité permanent P, de recommander et d'encourager l'enregistrement d'un motif suffisamment clair pour toutes les consultations. Si certains services ont rendu cette pratique obligatoire[28], beaucoup ne l'ont, semble-t-il, pas fait ou l'ont fait sans réel contrôle de l'application de cette mesure.

65. Il convient également de constater qu'à l'heure actuelle, les modalités d'enregistrement du motif de consultation n'incitent pas l'utilisateur du portail informatique policier à le faire. Son attention n'est, en effet, attirée que sur le fait que les consultations sont enregistrées et que des poursuites pénales et disciplinaires sont possibles en cas d'abus. Le champ « motif de consultation » n'est accessible qu'à partir d'une option offerte parmi d'autres en début de session.

- *Prévention technique*

66. De manière plus générale, il serait opportun de dégager, si possible, des solutions d'ordre informatique et technique permettant de prévenir les accès illégitimes aux bases de données, le plus efficacement possible et sans surcharge administrative pour l'utilisateur. Cette approche nécessite cependant une analyse de la part des services de police quant à la faisabilité de développer des solutions efficaces tant sur le plan technique que budgétaire compte tenu des priorités déjà arrêtées.

- *Pertinence de l'octroi des accès aux banques de données*

67. La responsabilité de l'octroi des accès aux banques de données appartient aux responsables policiers locaux et fédéraux. En particulier, les zones de police locale gèrent les accès à la BNG de manière autonome. Compte tenu de la philosophie de fonctionnement de la police intégrée, DRI fournit une aide aux responsables de la gestion et émet des « signaux » vers eux lorsque des situations problématiques sont détectées. Il n'existe donc pas, à proprement parler, de contrôle *sensu stricto* de l'octroi des accès.

68. L'octroi d'un accès à une base de données doit être réfléchi et individualisé, sans systématisme ou automatisme. Il ne peut être fondé sur le seul critère de la fonction exercée par le membre du service de police. Il doit tenir compte des situations et spécificités réelles du service de police et se limiter aux accès strictement nécessaires permettant aux membres des services de police de remplir leurs fonctions de manière efficace. La nécessité pour un membre des services de police de disposer *en permanence et individuellement* d'un accès à une base de données pour remplir concrètement ses missions de manière efficace devrait être un critère évalué régulièrement par les responsables policiers. Cette évaluation plus pointue ne peut être concrètement effectuée à partir de DRI.

[28] Par exemple, le directeur de l'information policière opérationnelle de la police fédérale (anciennement CGO) a prescrit dès 2009 à tous les membres de son service qui ont accès par leur fonction et pour l'exécution de leurs activités, de spécifier le motif de toute consultation effectuée dans les banques de données policières ou mises à la disposition des membres des services de police.

- *Exécution des contrôles*

69. L'approche des contrôles est en cours de révision au niveau de la police fédérale. Un processus de contrôle reposant sur une phase de détection de situations potentiellement suspectes suivie, si nécessaire, par des contrôles approfondis et ciblés portant sur les consultations litigieuses est plus opportun que celui reposant sur des vérifications de consultations sélectionnées de manière aléatoire en dehors de tout motif de suspicion. Une harmonisation du contrôle en ce sens pour l'ensemble de la police intégrée est souhaitable.

2.6.3. Répression des abus

70. Comme par le passé, le Comité permanent P continuera à dénoncer systématiquement aux autorités judicaires les plaintes et dénonciations qui lui sont adressées dans le cadre desquelles il existe des présomptions d'accès illégitimes aux banques de données. Le Comité permanent P ne peut que rappeler aux différents responsables policiers qu'ils doivent adopter la même politique lorsqu'ils détectent des abus, cela conformément aux prescrits de l'article 29 du Code d'instruction criminelle. Au niveau policier, il semble, en outre, judicieux de réfléchir à des mesures complémentaires de nature à renforcer le caractère dissuasif de la répression disciplinaire ou judiciaire afin d'éviter la récidive.

3. RÉACTIONS ET COMMENTAIRES DES PARTIES PRENANTES

3.1.1. Organe de contrôle de l'information policière

71. La problématique des accès aux banques de données, et plus particulièrement à la BNG, est une préoccupation majeure du COC. Les points les plus sensibles ressortant des observations effectuées au cours de la première partie de 2016 sont les suivants :

1) l'élaboration au niveau de la police intégrée d'une politique de consultation des banques de données en accord avec la LFP, la LVP (Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel sur la vie privée) et le code déontologie des services de police ;

2) la sensibilisation des membres du personnel aux consultations des banques de données ;

3) l'instauration d'un « *login* » obligatoire pour tout membre du personnel ainsi que l'obligation de mentionner la raison de la consultation ou du contrôle ;

4) le développement d'une politique cohérente relative à la gestion des accès tenant compte des principes du « *need to know* » plutôt que du « *nice to know* », cette politique devant également intervenir en matière de suppression des accès ;

5) la mise en œuvre de contrôles par les divers services à différents niveaux (local, supra local) mais aussi par les organes de contrôle compétents ;

6) l'accentuation du rôle et des tâches remplis par les fonctions centrales dans le cadre de la gestion et de la circulation de l'information : conseiller en sécurité, gestionnaires fonctionnels, chefs de corps de la police locale, services de contrôle interne et DRI ;

7) le rôle et la politique de DRI doivent être centraux et déterminants pour l'établissement des règles relatives aux accès et à la consultation des banques de données ;

8) le COC voit d'un bon œil les développements progressifs relatifs au SSO et à l'unification de la procédure des mots de passe ;

9) la directive relative à l'accès, à l'utilisation et au contrôle des moyens ICT de la police fédérale fera l'objet d'un examen attentif après sa parution.

72. En ce qui concerne les recommandations formulées par le Comité P, le COC souligne :

1) qu'outre le développement de mesures préventives et fonctionnelles sur le plan humain et technique par les services de la police locale et de la police fédérale, une mesure importante consiste en la mise en œuvre de contrôles réguliers tant internes qu'externes par les organes de contrôle compétents ;

2) que le rôle du conseiller en sécurité est essentiel ;

3) qu'il est indispensable d'avoir une identification univoque de l'utilisateur et l'insertion d'un motif de consultation valable dans tous les cas (sauf exceptions clairement limitées) pour toutes les applications. À cet égard, il semble aussi recommandé que l'accès en consultation ou en contrôle ne soit pas rendu possible à défaut de ces éléments. Enfin, les applications devraient se fermer automatiquement après un certain temps d'inactivité pour éviter leur utilisation abusive par autrui.

73. Le COC précise qu'il ne manquera pas de suivre l'évolution du dossier durant les mois à venir tout en soulignant que le suivi des accès et des consultations concerne également, en ce qui le concerne, la consultation des banques de données internationales et, surtout, la consultation de banques de données communes récemment créées au sein de certaines zones de police[29].

3.1.2. Police fédérale

74. La Commissaire générale souligne que les services de police ne sont jamais restés insensibles à la problématique et que les remarques du Comité P ne sont pas restées sans réaction et ce dès 2005. Réellement convaincue de la nécessité de continuer à lutter contre les usages abusifs des banques de données, elle veillera à aborder la problématique des accès ou consultations illégitimes pour l'ensemble des banques de données aussi bien opérationnelles qu'administratives mises à la disposition des services de police.

[29] Le COC fait référence à l'application « Infotheek » développée par la zone de police Westkust (outil informatique d'échange d'informations) pour laquelle il a rédigé un premier rapport intermédiaire début 2016.

75. La police fédérale émet quelques précisions et commentaires quant à certains points du rapport, plus particulièrement en ce qui concerne la finalité des contrôles effectués par la DRI. Les précisions et commentaire apportés ont été intégrés dans le texte même du rapport.

3.1.3. Commission permanente de la police locale

76. La CPPL se réjouit d'avoir été consultée quant au projet de rapport en espérant que cela contribuera au développement d'une organisation policière attachant une attention particulière à la garantie des droits et libertés constitutionnels de chacun en phase avec une société démocratique. Elle estime que le rapport donne un aperçu complet de la réglementation et des procédures existantes ainsi que des efforts aussi bien réactifs que préventifs entrepris pour prévenir et éradiquer les atteintes à la « *privacy* » du citoyen par un emploi illégitime des banques de données. Elle relève que le nombre d'infractions enregistrées ainsi que les suites qui en découlent sont très limités. La nature et le contexte dans le cadre duquel les infractions sont commises sont également peu connus. Elle précise aussi que la réaction en cas d'abus n'est généralement pas « compréhensive ».

77. Tenant compte de ce qui précède, la CPPL se montre fort préoccupée par le chiffre noir relatif au phénomène et le fait que les solutions proposées sont essentiellement de nature technique au niveau policier. Elle estime qu'elles ne contribueront pas à l'éradication des abus. Elle insiste également sur le fait que la consultation des banques de données fait partie des tâches élémentaires inhérentes au travail policier et que les autorités doivent se garder d'édicter des règles et procédures supplémentaires non conviviales. Le travail policier serait aussi compromis par un excès d'actions administratives de quelque nature que ce soit touchant la consultation des banques de données.

78. La CPPL note que l'aspect préventif qui se concrétise aujourd'hui par des '*infonews*', des messages et instructions publiés sans plus sur le 'Portal' ou la référence à des comportements attendus du personnel n'a qu'un impact limité sur le terrain. Il serait bien plus nécessaire de gérer les informations avec discernement. Celles-ci doivent être discutées verbalement et journalièrement. Dans une organisation policière centrée sur ses valeurs et consciente du pourquoi de son existence, le coaching et le suivi sur le terrain par les responsables policiers doivent avoir pour effet que l'emploi des banques de données de manière non abusive aille de soi pour les membres du personnel. Le message de la CPPL à cet égard peut se résumer en ces termes: « exprimer, discuter, convenir et interpeller ». Au sein de la police, l'accent est surtout mis sur l'aspect « exprimer » et cela de manière écrite. Une certaine attention est également portée à l'aspect « interpeller » mais de manière encore limitée actuellement. La CPPL n'est cependant pas favorable à une réaction exagérée de quelque sorte que ce soit. Elle plaide au contraire pour un investissement déterminé dans les aspects « discuter » et « convenir ». Ces aspects ne vont pas vraiment de soi dans la culture policière actuelle ni dans le cadre du fonctionnement habituel des services de police.

79. La CPPL relève enfin qu'il est beaucoup attendu de la nouvelle fonction de conseiller en sécurité. Elle note que pareille fonction n'est pas toujours considérée comme prioritaire en raison de l'orientation de la culture policière vers « l'opérationnel » ainsi que de l'impact budgétaire découlant de la mise en œuvre de la nouvelle fonction. L'organisation policière ne semble pas encline, non plus, à développer et à organiser une formation interne de sorte que les services de police ont tendance à aller chercher leur bonheur à l'extérieur de l'organisation policière dans le privé. Si cette voie est suivie, les services de police feront encore la chasse aux

coûts au détriment du travail spécifiquement policier. L'uniformité de l'approche et le contenu concret de la formation seront alors une illusion.

3.1.4. Considérations complémentaires du Comité permanent P

80. Le champ de l'enquête a été volontairement limité aux accès aux banques de données classiques utilisées par la majorité des membres des services de police lors de l'exercice de leurs activités ceux-ci étant en cause dans la quasi-totalité des dysfonctionnement connus. Cela n'exclut pas l'existence de dysfonctionnements dans le cadre de l'utilisation d'autres banques de données.

81. Il existe vraisemblablement un chiffre noir dont le niveau est impossible à évaluer actuellement. On peut raisonnablement penser que celui-ci résulte en grande partie de la difficulté de détecter les accès illégitimes « noyés » dans la masse des consultations parfaitement légitimes des banques de données. La probabilité que des dysfonctionnements ne soient détectés en l'absence de circonstances ou caractéristiques particulières les révélant est donc faible.

82. Même si elle peut toujours être améliorée, l'information existe depuis des années et est suffisamment claire pour que les membres des services de police soient bien au courant des limites en la matière. Chaque parution d'un bulletin d'information est l'occasion pour les responsables policiers de s'approprier la problématique. Tout dépend alors de la manière dont les informations sont traitées par ceux-ci. Une simple diffusion de l'information en se bornant à transmettre ou afficher les feuillets d'information n'est évidemment pas de nature à impacter durablement le personnel. Le Comité permanent P ne peut que souhaiter l'investissement actif des responsables policiers pour que le concept de « *privacy* » en général et dans le cadre de la consultation des banques de données en particulier soit intégré concrètement dans le fonctionnement policier ordinaire. Cela peut être réalisé sans attendre la mise en œuvre de structures spécifiques demandant des moyens qui ne sont pas forcément actuellement disponibles ou la formulation d'une recommandation spécifique. Beaucoup peut être fait sans moyens extraordinaires en allant au-delà de la simple attention occasionnelle portée au phénomène lorsqu'un dysfonctionnement est révélé ou lorsqu'un feuillet d'information paraît.

83. Les considérations précédentes démontrent effectivement l'importance de travailler sur l'aspect culturel. Les membres des services de police doivent être conscients du fait que la société et les citoyens se montrent de plus en plus soucieux de la préservation du droit à la « *privacy* ». Les atteintes à celui-ci par des personnes détentrices d'une fraction de l'autorité publique sont difficilement admissibles. L'intégration réelle du concept de « *privacy* » dans la culture policière constitue le meilleur rempart contre les abus. Certains corps et services développent ou ont déjà développés de louables initiatives en la matière. Il n'est donc pas indiqué de formuler une recommandation générale qui s'adresserait de manière uniforme à tous. La situation doit être analysée au niveau des différents corps de police locale et des services de police fédéraux. Les signes objectifs de prise en compte proactive de la problématique par les responsables policiers seront, sans nul doute, des « marqueurs » qui permettront d'évaluer la volonté d'intégrer la « *privacy* » dans la culture policière. À cet égard, la DRI entend bien mettre à l'avenir l'accent sur la responsabilisation et la conscientisation dans le cadre de la problématique.

84. Les recommandations émises dans le présent ne sont évidemment pas la panacée qui permettra d'éradiquer complètement et définitivement le phénomène. Le changement culturel

évoqué ci-avant ne peut être espéré à court terme de sorte qu'il est nécessaire de l'accompagner d'un dispositif visant à entraver, autant que faire se peut, l'usage abusif des banques de données. Ce dispositif vise essentiellement à limiter les possibilités d'abus tout en veillant à ne pas porter atteinte à l'opérationnalité de la police ou à occasionner de surcharge administrative au niveau des intervenants de terrain. Les recommandations sont suffisamment nuancées, souples et adaptables que pour permettre aux responsables policiers d'appréhender la problématique en fonction de la situation réelle sur le terrain sans réaction excessive et sans pénaliser la toute grande majorité des membres des services de police qui ne tombent pas dans les travers combattus. Le Comité permanent P plaide évidemment pour que les moyens nécessaires puissent être libérés dans le futur pour la mise en œuvre concrète de la nouvelle structure policière spécifique prévue dans le cadre de la « *privacy* » ainsi que pour la mise en œuvre rapide d'une formation interne à la police destinée aux futurs conseillers en sécurité et en protection de la vie privée.

85. Pour l'essentiel , le Comité permanent P adhère aux considérations et commentaires des parties prenantes consultées. Il fait plus spécifiquement siennes les considérations et recommandations émises par le COC ayant trait à la nécessité d'identifier l'utilisateur de manière univoque, l'introduction d'un motif de consultation valable (sauf exceptions clairement limitées) pour toutes les applications et la fermeture automatique des applications après un certain temps d'inactivité pour éviter l'utilisation abusive au nom d'autrui. La dynamique constatée au niveau de la police fédérale dans le cadre de la problématique devrait être mise à profit pour développer les initiatives nécessaires à la concrétisation des recommandations susceptibles d'améliorer la situation en concertation avec la police locale.

4. CONCLUSIONS

86. Les consultations illégitimes connues de banques de données mises à la disposition des services de police sont essentiellement commises en dehors du cadre professionnel. Elles sont toutes potentiellement attentatoires à la vie privée du citoyen.

87. L'examen du dispositif en place visant à lutter contre ce phénomène montre que :

1) les mesures prises sur le plan de la sensibilisation et de l'information des membres des services de police paraissent suffisantes ;

2) l'enregistrement du motif de la consultation est fortement recommandé mais n'a toujours pas de caractère obligatoire sauf en ce qui concerne la consultation des photos du RRN. Cette pratique constitue cependant un frein aux consultations abusives, responsabilise les membres des services de police et facilite les éventuelles enquêtes et la justification des accès aux bases de données ;

3) plusieurs éléments militent pour une évolution du système de contrôle *a posteriori* actuel: caractère peu opportun de contrôles reposant sur la vérification de la légitimité de consultations sélectionnées de manière aléatoire en vue de sensibiliser les responsables policiers, impact sur la sensibilisation des responsables policiers ayant vraisemblablement peu d'effet de rémanence, probabilité très faible d'être soumis à un contrôle pour les membres des services de police ayant commis un accès illégitime et donc aspect dissuasif assez limité, responsabilisation des services de police locaux perfectible en raison de la

centralisation du contrôle au niveau de la police fédérale qui a, par ailleurs, entamé une réflexion à ce sujet ;

4) un contrôle portant sur l'octroi de l'accès aux banques de données n'existe pas *sensu stricto*. La DRI fournit une aide aux responsables policiers en émettant des « signaux » lorsque des situations problématiques sont détectées. La pertinence de l'octroi d'accès permanents aux bases de données doit être évalué en tenant compte des spécificités des différents services de police et des missions réellement prestées par les membres du personnel.

5. RECOMMANDATIONS

5.1. Mesures préventives

88. Il est indispensable que les responsables policiers procèdent à un examen *critique et individualisé* lors de l'octroi des autorisations d'accès aux bases de données. Cet examen critique devrait être réalisé non seulement d'initiative en cas de changement de fonction ou de modification dans l'attribution des missions des membres du personnel mais aussi régulièrement (par exemple lors de l'évaluation du personnel). Les responsables devraient s'assurer que les membres de leur personnel ont *effectivement et concrètement* besoin, en fonction des spécificités du service de police, des contraintes organisationnelles et des missions réellement exécutées, de *disposer en permanence et individuellement* des accès aux bases de données.

89. Compte tenu des avantages que procure l'enregistrement du motif de la consultation, il paraît opportun de rendre cette pratique obligatoire pour toutes les consultations des banques de données au sein de la police intégrée tout en prévoyant la possibilité pour les responsables policiers d'y déroger limitativement et de manière motivée afin de pouvoir répondre aux spécificités ou contre-indications existant au sein de leur service. Ces dérogations motivées pourraient être accordées temporairement ou de manière permanente, pour la consultation de toutes ou certaines bases de données, dans des circonstances ou missions spécifiquement déterminées. L'obligation d'enregistrer dans le champ « motif de consultation » un élément permettant d'identifier univoquement le membre du personnel qui demande une consultation par l'intermédiaire d'un collègue devrait également être immédiatement généralisée. Dans cette perspective, la facilitation de l'enregistrement du motif de consultation afin de rendre la pratique plus évidente et conviviale serait une plus-value (amélioration de l'interface de consultation des banques de données).

90. Le développement de la prévention informatique et technique en vue de prévenir les accès illégitimes est souhaitable. Il pourrait s'agir, entre autres, de proposer à l'utilisateur du portail informatique policier le remplissage du champ « motif de consultation » avant la consultation proprement dite, de prévoir l'identification du demandeur réel d'une consultation ou de limiter l'accès aux bases de données aux entités codées dans un dossier ouvert dans l'ISLP.

91. La prise de mesures spécifiques par les responsables policiers visant à prévenir la récidive des membres des services de police reconnus coupables d'avoir accédé illégitimement à une base de données permettrait d'accroître l'efficacité de la répression en la matière. Il pourrait

s'agir, par exemple, du retrait de l'autorisation d'accès *direct* à une ou plusieurs banques de données pour une certaine durée ou de l'exécution par les responsables policiers de contrôles *a posteriori* visant le membre du personnel concerné pendant une certaine période.

5.2. Mesure de contrôle

92. L'exécution de contrôles *a posteriori* devrait être rendu obligatoire par chaque corps et service de la police intégrée. Les principes et grandes lignes de ces contrôles devraient faire l'objet d'une concertation entre les composantes de la police intégrée en s'inspirant de la directive de la police fédérale entrant prochainement en vigueur. Les caractéristiques essentielles suivantes devraient se retrouver dans cette nouvelle approche :

1) les contrôles devraient s'exercer dans le respect des principes généraux de finalité, de proportionnalité, de subsidiarité et de transparence ;

2) les contrôles devraient être réalisés régulièrement et d'initiative par les services de police locaux et fédéraux avec l'appui de DRI afin de tenir compte des spécificités inhérentes à chaque service de police. Chaque membre du personnel devrait être repris régulièrement dans la procédure de contrôle afin d'augmenter significativement le risque de détection d'accès illégitime. Les membres du personnel exonérés de l'obligation d'enregistrer un motif de consultation devraient également y être soumis afin de vérifier qu'ils n'abusent pas de cette facilité et que les limites de l'exonération octroyée sont bien respectées. La fréquence de contrôle devrait être déterminée en fonction de la taille de chaque service ou corps de police et en fonction de l'appui pouvant être fourni par la police fédérale. L'organisation de ces contrôles pourrait être idéalement confiée aux futurs conseillers en sécurité et en protection de la vie privée ;

3) les modalités concrètes et pratiques d'enregistrement des motifs de consultation devraient être fixées au niveau des différents corps de police locale et services de police fédéraux de sorte qu'ils soient non seulement pertinents et « parlants » pour les contrôleurs mais aussi pour les membres des services de police afin qu'ils puissent justifier facilement leurs consultations en cas de besoin (fonction d'aide-mémoire performante) ;

4) le contrôle proprement dit devrait reposer sur un examen général des consultations visant à détecter d'éventuelles situations anormales sur base de critères et d'indicateurs pertinents. Les indicateurs de possibles accès illégitimes pourraient être déterminés de manière générale mais aussi en fonction de la situation et des spécificités des corps ou des services de police. Des indicateurs devraient également être déterminés sur base d'une analyse critique des activités professionnelles afin de détecter d'éventuelles pratiques illégitimes non toujours forcément évidentes pour les membres des services de police et, peut-être, exécutées de manière routinière (par exemple l'exécution de contrôles en BNG dans le cadre de dossiers administratifs). De manière non exhaustive, les éléments suivants pourraient, par exemple, constituer des indicateurs susceptibles d'entraîner un contrôle plus approfondi des consultations d'un membre des services de police soumis au contrôle :

- absence d'enregistrement d'un motif de consultation alors que le membre du service de police n'a pas été exempté de cette obligation par les responsables policiers ;
- inscription d'un motif de consultation insuffisamment pertinent ou parlant en contradiction avec le prescrit local ;
- exécution d'un nombre anormal de consultations ;
- exécution de consultations à des heures anormales par rapport aux prestations de service du membre du personnel contrôlé ;
- consultations ayant pour objet d'autres membres du personnel de la zone ou du service de police auquel appartient le membre du personnel ;
- consultations ayant pour objet des responsables politiques locaux, des personnalités locales ;

5) si des situations potentiellement anormales sont détectées, des contrôles ciblés approfondis des consultations litigieuses devraient alors être effectués. Ceux-ci consisteraient en des demandes de justification adressées aux membres du personnel concernés en vue d'établir leur légitimité.

5.3. Concrétisation

93. Il est souhaitable que les recommandations formulées soient rendues opposables à l'ensemble des corps et services de la police intégrée. Cet objectif pourrait être atteint, par exemple, en les intégrant dans la directive MFO-3.

6. SUIVI

94. La mise en place des conseillers en sécurité et en protection de la vie privée et de la plate-forme de la sécurité et de la protection des données constitue une opportunité pour les services de police de mettre en place une réflexion structurée et le développement d'une véritable politique visant, notamment, à prévenir les consultations illégitimes des banques de données. Bien qu'aucune situation actualisée ne soit disponible à l'heure actuelle, il semble bien que le déploiement de ce nouveau dispositif est loin d'être terminé au sein des services de police. Un problème de moyens entrave, en particulier, la mise en place de la plate-forme de la sécurité et de la protection des données. L'offre en formation spécifique a fait l'objet de recherches mais n'a pu encore être concrétisée.

95. Le Comité permanent P entend effectuer un suivi attentif de la manière selon laquelle les services de la police intégrée développent et mettent en œuvre une politique de sécurisation et de protection de la vie privée. Ce suivi sera, plus particulièrement, l'occasion de s'assurer de la prise en compte des recommandations formulées en matière de lutte contre les accès illégitimes aux banques de données.

96. ANNEXE

97. La liste des abréviations utilisées.

ANNEXE

ABRÉVIATIONS UTILISÉES

Abréviation	Signification
BNG	Banque de données nationale générale
CALog	Cadre administratif et logistique de la police
CPPL	Commission permanente de la police locale
CPVP	Commission de la protection de la vie privée
DGR	Direction générale de la gestion des ressources et de l'information de la police fédérale
DIV	Direction de l'immatriculation des véhicules
DRI	Direction de l'information policière et des moyens ICT de la police fédérale
FEEDIS	'*Feeding Information System*' – Application informatique utilisée au sein de la police fédérale
ICT	'*Information and Communication Technology*'
ISLP	'*Information System for Local Police*' – Système informatique policier utilisé dans les zones de police locale
LFP	Loi du 5 août 1992 sur la fonction de police
LVP	Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel
MFO-3	Directive commune MFO-3 du 14 juin 2002 des ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative
PORTAL	Portail informatique policier
RCA	Registre central des armes
RRN	Rijksregister / Registre National
RPO	Application « Numéros de plaques incomplets »
SCHEVAL	'*Schengen Evaluation Working Group*'
SICAD	Service d'information et de communication d'arrondissement
SIDIS	Système d'information des détentions / Detentie-informatiesysteem
SSO	'*Single Sign On'* – Adaptation technique visant à harmoniser les '*logins*' informatiques de la police