

# CONTRÔLE THÉMATIQUE

**RAPPORT DU CONTRÔLE THÈMATIQUE DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE CONCERNANT L'ÉCHANGE D'INFORMATIONS DE LA POLICE AVEC LES PARTENARIATS LOCAUX DE PRÉVENTION (PLP)**

## RAPPORT

*Référence : CON20012*



1. INTRODUCTION 1
2. LES COMPÉTENCES DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE 1
3. OBJET DU CONTRÔLE ET MÉTHODOLOGIE 3
4. UN PARTENARIAT LOCAL DE PRÉVENTION : LE CADRE JURIDIQUE 5
5. CONCLUSIONS DE L'ENQUÊTE 5
5.1. La représentativité de l'enquête 5
5.2. Résultats des visites sur place 5
6. CONCLUSION ET RECOMMANDATION 7

* * * * * *

## 1. INTRODUCTION

1. Dans le cadre de ses compétences de contrôle, l'Organe de contrôle de l'information policière ('Organe de contrôle' ou 'COC') a décidé de mener une enquête de contrôle auprès de la police locale dans le cadre d'un 'contrôle thématique'[1] concernant l'échange d'informations de la police avec les partenariats locaux de prévention (en abrégé PLP).

Le présent rapport fait état des conclusions de ce contrôle et en particulier des visites sur place.

## 2. LES COMPÉTENCES DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

2. La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[2] a réformé l'Organe de contrôle en une autorité de contrôle à part entière en plus des compétences de contrôle en matière de gestion de l'information policière prévues par la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1er et les Titres 2 et 7 de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/14 inclus de la LFP, relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de la gestion de l'information et de l'intervention policière. En vertu de la réglementation susmentionnée, le COC dispose dès lors d'une compétence de surveillance générale à l'égard de tous les traitements de données (à caractère personnel) opérationnels et non opérationnels effectués par la GPI.

Pour ce qui est de la mission de contrôle, l'Organe de contrôle est chargé du contrôle du traitement des informations et des données visées à l'article 44/1 de la LFP, y compris celles introduites dans les banques de données visées à l'article 44/2, ainsi que de toute autre mission qui lui est confiée par ou en vertu d'autres lois.

L'Organe de contrôle est en particulier chargé du contrôle du respect des règles relatives à l'accès direct à la Banque de données nationale générale (BNG) et à sa consultation directe, ainsi que du respect de l'obligation visée à l'article 44/7, 3e alinéa de la LFP, qui oblige tous les membres des services de police à alimenter cette banque de données.

À travers un contrôle du fonctionnement, l'Organe de contrôle vérifie si le contenu de la BNG et la procédure de traitement des données et informations qui y sont conservées sont conformes aux dispositions des articles 44/1 à 44/11/14 de la LFP et à leurs mesures d'exécution.

---

[1] Le COC établit une distinction entre différentes formes de contrôles ou de surveillance. Le COC procède soit à :
- **un contrôle global :** il s'agit d'un contrôle qui s'assortit d'une ou plusieurs visites approfondies sur place et d'une portée très large ;
- **un contrôle thématique :** comme le nom l'indique, il s'agit d'une enquête menée sur un thème déterminé et qui peut inclure à la fois de la *desk research* et des visites sur place ;
- **un contrôle technique :** il s'agit d'un contrôle qui se concentre sur la licéité, l'exhaustivité et l'exactitude des enregistrements/traitements effectués dans les banques de données policières ;
- **un contrôle restreint :** ce contrôle porte sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier ;
- **un contrôle international :** il s'agit des éventuelles enquêtes internationales auxquelles le COC apporte son concours ;
- **un contrôle spécial :** il s'agit d'un contrôle portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme.

[2] M.B. 5 septembre 2018. Cette loi contient des dispositions qui donnent exécution au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après dénommé « RGPD », et à la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après dénommée « directive Police-Justice » ou LED (**L**aw **E**nforcement **D**irective)).

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MAP »[3]. Conformément à l'article 46/6 de la LFP, toute autorisation et prolongation d'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée à l'Organe de contrôle sauf lorsque l'utilisation des caméras est réalisée sous le contrôle d'un magistrat. L'Organe de contrôle doit alors examiner si les conditions pour la décision, la prolongation ou l'exécution de cette mesure sont remplies.

L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé[4]. Les membres et les membres du personnel de l'Organe de contrôle[5] disposent à cet égard de compétences d'investigation, après quoi le comité de direction de l'Organe de contrôle peut, en marge des requêtes et recommandations qu'il formule, prendre également des mesures correctrices[6], ces dernières en tant que *« ultimum remedium »* lorsque le COC constate des infractions à la réglementation en vigueur.

Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du 15 mai 2007 *« sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police »* et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016 *« relative au traitement des données des passagers »*, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/14 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[7].

L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 *« modifiant diverses dispositions relatives au traitement des données des passagers »*.

Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE')[8], de la validation (ou non) des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

Un recours juridictionnel peut être introduit dans les trente jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire[9].

## 3. OBJET DU CONTRÔLE ET MÉTHODOLOGIE

3. La circulaire ministérielle du 28 février 2019 régit la mise en place et le fonctionnement des partenariats locaux de prévention (PLP)[10]. Un partenariat local de prévention (PLP) est un accord de collaboration structuré entre les citoyens, la police locale et les autorités administratives, dans le cadre duquel le citoyen est impliqué dans la prévention de la criminalité, la lutte contre la criminalité et le renforcement du sentiment de sécurité dans la commune, notamment en échangeant des informations avec la police. Plusieurs PLP peuvent être créés au sein d'une même commune[11]. Selon une réponse formulée le 9 mars 2023 par le ministre de l'Intérieur à une question parlementaire, 1.319 PLP avaient dans l'intervalle été créés en Belgique.

---

[3] MAP signifie « ***M**éthodes **A**dministratives **P**articulières* ».
[4] Art. 240, 4° de la LPD.
[5] À savoir les membres du personnel du **D**ienst **O**nderzoeken / **S**ervice d'Enquête (DOSE) et du secrétariat, c'est-à-dire des juristes et des experts en matière de TIC.
[6] Art. 244 (compétences d'investigation des membres et des membres du personnel) et 247 de la LPD (mesures correctrices à prendre par le comité de direction (DIRCOM) du COC).
[7] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[8] Telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (*M.B.* du 8 août 2022).
[9] Art. 248 de la LPD.
[10] Voir notamment www.besafe.be/fr/partenariat-local-de-prevention-plp et plus spécifiquement pour la circulaire : https://www.besafe.be/sites/default/files/2022-10/circulaire_plp.pdf.
[11] Cela peut par exemple aussi être le cas dans un certain secteur. Il existe ainsi notamment un PLP-I, un partenariat local de prévention pour les indépendants (commerçants).

4. Afin de se faire une idée des informations qui sont échangées par la police avec un PLP, de la manière dont ces informations sont échangées et des conventions qui sont passées avec un PLP, il a été procédé à un contrôle thématique.

5. L'enquête s'est déroulée en cinq étapes :

1) un questionnaire qui serait transmis aux zones de police sélectionnées a été établi ;
2) une sélection des zones de police qui seraient soumises à une visite sur place a été opérée ;
3) le plan de communication des zones de police sélectionnées a été demandé ;
4) une visite sur place a été effectuée auprès des zones de police sélectionnées ;
5) les conclusions de l'enquête ont été compilées dans le présent rapport.

6. Pour des raisons de lisibilité et de capacité, il n'a donc pas été opté pour une consultation générale de toutes les zones de police au sein desquelles un ou plusieurs PLP a (ont) été mis en place.

7. Les questions soumises lors de la visite sur place ont été réparties en deux volets.

7.1. En ce qui concerne les informations provenant d'un PLP

- L'objectivité et la pertinence des informations fournies par un PLP à la police sont-elles évaluées ?
- Où sont enregistrées les informations fournies par un PLP à la police ?
- Quel est le délai de conservation des informations fournies par un PLP à la police ?

7.2. En ce qui concerne les données policières fournies par la police à un PLP

- Comment faut-il faire concrètement la distinction entre les messages urgents et les messages non urgents ?
- Une distinction est-elle faite entre les données à caractère personnel et les informations ?
- Quel canal de communication est utilisé ?
- Existe-t-il une description du processus de travail concret ?
- Tient-on à jour un aperçu documenté des informations communiquées à un PLP ?
- Est-il procédé à un contrôle interne et les résultats du contrôle sont-ils documentés ?
- Une note interne a-t-elle été établie à ce sujet au niveau du corps ?
- Ce traitement est-il enregistré dans un registre des traitements (par ex. RegPol) ?

8. Les zones de police qui ont été soumises à une visite sur place ont été sélectionnées sur la base de trois critères. Le premier critère était le nombre de PLP présents dans les Régions, exprimé en pourcentage. Selon une étude menée par l'UGent en 2020, 80 % des PLP se situent en Région flamande, 19 % en Région wallonne et 1 % en Région de Bruxelles-Capitale[12]. Pour des raisons pratiques et organisationnelles, la Région wallonne et la Région de Bruxelles-Capitale ont été regroupées.
Le deuxième critère tenait compte de la catégorie des zones de police. Le critère 'catégorie' renvoie au nombre de membres du personnel des zones de police[13]. La sélection opérée était donc un mélange de zones de police des différentes catégories.
Enfin, la priorité a été dans la mesure du possible accordée aux zones de police qui n'avaient encore jamais été soumises par le COC à une visite sur place.

À la lumière de ce qui précède, quatre (4) zones de police ont été sélectionnées en Région flamande et (2) en Région wallonne.

## 4. UN PARTENARIAT LOCAL DE PRÉVENTION : LE CADRE JURIDIQUE

9. La mise en place et le fonctionnement d'un PLP sont associés à un certain nombre d'exigences administratives formelles qui sont énoncées dans la circulaire ministérielle *« relative aux Partenariats locaux de Prévention »* du 28 février 2019 (ci-après 'la circulaire PLP'). Pour le traitement des données à caractère personnel, cette circulaire renvoie

[12] W. HARDYNS, L. PAUWELS, T. SNAPHAAN, *Buurtinformatienetwerken en lokale veiligheid. Een evaluatiestudie op basis van een mixed-method experimenteel design* (Executive summary), 2020, SPF Intérieur, Direction générale Sécurité et Prévention ; voir aussi www.besafe.be/fr/partenariat-local-de-prevention-plp/partenariats-locaux-de-prevention-et-la-securite-locale.

[13] Voir l'article 67 de la loi du 26 avril 2002 relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police. Il existe 5 catégories en ce qui concerne la police locale, la catégorie 1 regroupant les zones de police comptant moins de 75 membres du personnel employés à temps plein, la catégorie 2 regroupant les zones de police comptant au moins 75, mais moins de 150 membres du personnel employés à temps plein, la catégorie 3 regroupant les zones de police comptant au moins 150, mais moins de 300 membres du personnel employés à temps plein, la catégorie 4 regroupant les zones de police comptant au moins 300, mais moins de 600 membres du personnel employés à temps plein et la catégorie 5 regroupant les zones de police comptant au moins 600 membres du personnel employés à temps plein.

au discours du droit de la protection des données qui prévoit que les modalités de l'échange d'informations soient énoncées dans un plan de communication[14]. Le plan de communication distingue deux flux de données : d'une part la communication d'un PLP à la police, et d'autre part la communication de la police à un PLP. Dans ce dernier flux, une distinction est faite entre les messages *« urgents »* ou *« chauds »* et les messages *« non urgents »* ou *« froids »*[15].

10. Selon l'article 9 de la circulaire PLP, les messages urgents (ou chauds) contiennent des informations qui peuvent être pertinentes pour un PLP. Les messages non urgents (ou froids) sont des *« messages de feed-back ou de prévention »*. Les systèmes de communication utilisés sont également mentionnés dans le plan de communication[16]. L'article 9 de la circulaire PLP ne précise cependant pas quel peut ou doit être le contenu des messages respectifs qui sont transmis par la police à un PLP.

11. Il est par conséquent important d'examiner comment la police donne forme à l'échange d'informations avec un PLP. La formulation vague de la circulaire PLP et son silence juridique quant au fondement juridique de ces communications font en effet que chaque zone de police participante peut ou doit évaluer elle-même quelles données policières (données à caractère personnel et informations) sont partagées avec un PLP et quels canaux sont utilisés pour ce faire. Dans la pratique, le chef de corps dispose donc sur ce plan d'une grande autonomie (au sens d'absence de supervision centrale de la part de l'autorité de tutelle de la police) qui a un impact sur le traitement des données et sur la manière dont ce traitement des données est (ou non) contrôlé en interne.

## 5. CONCLUSIONS DE L'ENQUÊTE

### 5.1. La représentativité de l'enquête

12. Il convient de faire remarquer au préalable que les résultats exposés ci-après ne peuvent pas être tout bonnement extrapolés à tous les PLP enregistrés, principalement parce que le nombre de PLP enregistrés ne dit rien ou pas grand-chose quant à leur **opérationnalité réelle**. Par 'opérationnalité réelle', on entend un PLP qui est actif et qui fonctionne comme le stipule la circulaire PLP. En conséquence, les conclusions énoncées dans le présent rapport ne sont pas représentatives de tous les PLP enregistrés. À l'inverse, cette remarque vaut également pour les zones de police au sein desquelles un PLP a été mis en place, mais qui n'ont pas été soumises à une visite sur place.

### 5.2. Résultats des visites sur place

13. Il apparaît que sur les six (6) zones de police visitées, il n'y en a que deux au sein desquelles un ou plusieurs PLP est (sont) réellement opérationnel(s). Dans les quatre autres, les PLP existent seulement sur papier. Comme nous le verrons plus loin, les deux zones de police en question disposent d'un système et d'une documentation performants traduisant bien les objectifs de la circulaire PLP.

14. En ce qui concerne le traitement des données, une distinction claire est perceptible entre d'une part le flux entrant d'informations du PLP, qui relève de l'application du règlement général sur la protection des données (RGPD), et d'autre part le flux sortant, à savoir le traitement des données transmises par la zone de police aux membres du PLP, lequel relève du titre 2 de la LPD et de la LFP.

15. Les deux zones de police disposent de directives internes et d'un plan de communication concernant la collaboration avec un PLP.

16. Une équipe de fonctionnaires de police composée à cette fin s'occupe spécifiquement de la collaboration avec les PLP.

5.2.1. <u>Les notifications transmises par un PLP</u>

17. Une distinction est faite entre les messages urgents et les messages non urgents (froids). Les premiers visent la communication de faits punissables et de personnes disparues ou de disparitions inquiétantes (enfants, personnes âgées), tandis que la deuxième catégorie de messages a trait à la prévention et aux phénomènes. Pour ces messages, il est crucial de fournir un description physique le plus exact et le plus complet possible de l'auteur (présumé) ou de la personne suspecte/disparue. En soi, il s'agit de faits punissables, d'agissements suspects ou de personnes disparues pouvant être déclaré(e)s ou signalé(e)s à la police par tout citoyen. L'une des zones de police mise dans ce contexte

[14] Art. 9 de la circulaire PLP.
[15] Ibid.
[16] Ainsi que dans la charte qui est signée par les parties concernées (bourgmestre, chef de corps et coordinateur PLP) et qui est approuvée par le SPF Intérieur (art. 6 de la circulaire PLP). Ce document n'est pas pris en considération dans le cadre du contrôle étant donné qu'il ne contient pas de conventions concrètes concernant le contenu des informations et les modalités exactes de l'échange.

résolument sur l'utilisation de BE-Alert par les PLP et sur la manière dont cette application doit être utilisée. La zone de police insiste auprès du PLP sur le fait qu'il n'est pas un service de police et dispose encore moins de compétences de police.

5.2.2. Le traitement des notifications par la zone de police

19. Parmi les notifications qui lui parviennent, la zone de police examine d'abord s'il y a suffisamment d'éléments pour pouvoir activer un PLP. Dans l'affirmative, les informations sont transmises aux membres du PLP. La nature des informations qui sont transmises aux membres du PLP dépend de la situation concrète. Les membres du PLP peuvent par exemple être priés de prêter attention à une personne répondant à une description physique donné et/ou se déplaçant dans une certaine direction. Cette communication aux membres du PLP peut aussi s'assortir de mesures préventives à prendre.

20. Les notifications que la zone de police reçoit du PLP suivent le processus de traitement classique qui est appliqué pour chaque notification. Une fiche de description physiqueet, le cas échéant, une fiche d'intervention sont créées. Lorsque les faits matériels sont actés dans un procès-verbal, son traitement suit le processus d'enregistrement et de validation (légal) normal qui est prévu par la LFP et par la directive MFO-3[17].

21. Le système de traitement permet toutefois de distinguer les notifications ordinaires des notifications d'un PLP. De cette manière, la zone de police peut assurer un suivi spécifique des incidents notifiés par les PLP, identifier les phénomènes et les tendances et adapter, actualiser et optimaliser la collaboration avec les PLP.

22. Il découle donc de ce qui précède que l'on applique pour le traitement des notifications effectuées par un PLP le même processus de traitement dans l'environnement policier que pour n'importe quelle déclaration ou notification, par un citoyen, d'un fait punissable ou suspect ou d'une personne disparue.

5.2.3. Le traitement de données

23. Le COC a eu l'occasion lors de la visite sur place d'accéder à une liste des notifications envoyées aux membres du PLP en 2023. Cela a permis de constater l'attention qui est accordée à la casuistique de la communication et des données (à caractère personnel) en fonction du contexte spécifique et des circonstances de la communication aux membres du PLP.

24. D'autre part, la description physiquequi est transmis aux membres du PLP peut contenir les données (caractéristiques) suivantes :
- sexe
- âge
- langue
- taille
- poids
- corpulence
- cheveux (couleur)
- couleur de peau
- yeux/lunettes
- tatouages
- cicatrices
- tenue vestimentaire.

25. Il s'agit donc d'une description détaillée des caractéristiques personnelles de la personne concernée (disparue) ou de l'auteur présumé ou suspect. La communication de ce signalement n'est toutefois pas mentionnée dans la circulaire, d'une part, et est d'autre part un traitement qui relève de l'application du titre 2 de la loi relative à la protection des données et de la LFP.

Il semble que pour disposer d'un point de repère objectif et juridique, il soit possible et nécessaire, avec un peu de bonne volonté et moyennant une interprétation extensive, de lire la circulaire PLP conjointement avec le régime prévu pour les avis de recherche qui peuvent être publiés par la police ou par le ministère public, à savoir la directive ministérielle *« concernant la diffusion d'avis de recherche judiciaires dans les médias et sur Internet »*[18] et la circulaire COL 7/1999 du 30 avril 1999 intitulée *« Informations qui peuvent être transmises à la presse par les autorités judiciaires et les services de police durant la phase de l'enquête préparatoire »*[19].

[17] Directive commune MFO-3 des ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative.
[18] *M.B.* 1er juillet 2005.
[19] https://www.om-pm.be.

## 6. CONCLUSION ET RECOMMANDATION

26. Le nombre limité de PLP ayant fait l'objet d'une visite sur place n'est pas dû uniquement à la capacité opérationnelle et aux ressources limitées de l'Organe de contrôle, mais aussi au nombre limité de PLP réellement opérationnels au regard de l'esprit et des objectifs de la circulaire du 28 février 2019 relative aux Partenariats locaux de Prévention.

27. Il convient à cet égard de faire remarquer que ces résultats très limités ne permettent pas de déduire que d'autres zones de police n'ayant pas été visitées soient responsables de l'absence d'un PLP réellement opérationnel. L'initiative de lancer un PLP incombe avant tout au citoyen, qui doit donc avoir l'intention et la maturité de (pouvoir et vouloir) réaliser les objectifs de la circulaire du 28 février 2019. D'autre part, la zone de police doit disposer des ressources et de la capacité policière requises pour faciliter et perpétuer suffisamment la collaboration.

28. Cette volonté était clairement présente dans deux des six zones de police visitées, qui ont fourni à l'Organe de contrôle des réponses satisfaisantes à toutes les questions de l'enquête que nous énoncions au point 7 du présent rapport.

29. Par ailleurs, il est apparu que l'affectation de ressources et de capacité par la zone de police dépend notamment aussi de la maturité du PLP.

30. En ce qui concerne la manière dont les données sont traitées par les zones de police, les processus de travail appliqués sont les mêmes que pour n'importe quelle notification ou déclaration (urgente) d'une infraction ou d'une disparition (inquiétante) qui est faite par un citoyen. Dans deux zones de police, il était possible de mesurer individuellement les notifications effectuées dans le cadre d'un PLP, ce qui permet évidemment de contrôler et de surveiller l'efficacité et la qualité du fonctionnement du PLP et de la police.

31. L'enquête démontre toutefois aussi que la circulaire du 28 février 2019 ne précise pas quel signalement un PLP peut communiquer à la zone de police, ni surtout quelles données à caractère personnel la zone de police doit ou peut le cas échéant communiquer aux membres du PLP. Bien que la directive ministérielle susmentionnée et la circulaire COL 7/1999 offrent certains points de repère, une recommandation au ministre compétent s'impose dans l'intérêt de la sécurité juridique.

## PAR CES MOTIFS,

## l'Organe de contrôle de l'information policière,

**<u>Recommandation</u>**

L'Organe de contrôle ordonne au ministre de l'Intérieur :

1) **<u>à titre principal</u>**, d'adapter la loi sur la fonction de police du 5 août 1992 afin de conférer un fondement juridique solide à la communication, par la police, de données à caractère personnel et d'informations aux (participants des) partenariats locaux de prévention (à insérer dans la sous-section 8 de la section 12 du chapitre IV) ;
2) au moins, **<u>à titre subsidiaire</u>**, d'actualiser ou d'adapter la circulaire du 28 février 2019 relative aux Partenariats locaux de Prévention en fonction du titre 2 de la loi du 30 juillet 2018 *« relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel »* et de la loi du 5 août 1992 *« sur la fonction de police »*, afin :
    a. de mentionner explicitement dans la circulaire le fondement juridique de l'échange d'informations entre la zone de police et le PLP ;
    b. de déterminer le signalement et, le cas échéant, les données à caractère personnel qui peuvent être communiqués par la zone de police aux membres du PLP dans le cadre de la finalité spécifique de la circulaire.

Rapport approuvé par l'Organe de contrôle de l'information policière le 18 juin 2024.

Copie :

- au ministre de l'Intérieur,
- au ministre de la Justice,
- au président du Collège des procureurs généraux,
- au président du Conseil des procureurs du Roi,
- au président de la Commission Permanente de la Police Locale,
- au président du Conseil Fédéral de Police,
- au président du Conseil des Bourgmestres.

Pour l'Organe de contrôle,

Frank SCHUERMANS
Président *a.i.*
(Sé)