ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA200006		15/09/2020

Objet : **Avis relatif à la proposition de loi modifiant diverses dispositions concernant l'approche administrative et portant création d'une direction chargée de l'évaluation de l'intégrité des pouvoirs publics (DOC 55 1381/001).**

L'Organe de contrôle de l'information policière (ci-après 'le COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après la 'Loi sur la protection des données' ou 'LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après dénommée en abrégé la 'Loi organique APD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après la 'LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après la 'LED').

Vu la loi du 25 décembre 2016 relative au traitement des données des passagers.

Vu la demande du 17 juillet 2020 de Monsieur Ortwin Depoortere, président de la Commission Intérieur, Sécurité, Migration et Matières administratives du parlement fédéral, d'émettre un avis sur la proposition de loi susmentionnée (ci-après « la proposition de loi ») pour le 18 septembre 2020.

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 15 septembre 2020, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a profondément modifié les tâches et les missions de l'Organe de

[1] 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 ou « RGPD »).

[2] 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*

contrôle. L'article 4 §2, quatrième alinéa de la loi organique du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après la « Loi organique APD ») dispose que pour les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est également compétent lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socio-économiques ou de traitements de ressources humaines. L'Organe de contrôle doit être consulté dans le cadre de la préparation d'une législation ou d'une mesure réglementaire liée au traitement de données à caractère personnel par les services de police de la police intégrée (voir l'article 59 §1er, 2e alinéa et l'article 236 §2 de la LPD ainsi que l'article 36.4 du RGPD et l'article 28.2 de la Directive Police et Justice). Dans ce cadre, l'Organe de contrôle a pour mission d'examiner si l'activité de traitement envisagée par les services de police est conforme aux dispositions des Titres 1er (pour les traitements non opérationnels)[3] et 2 (pour les traitements opérationnels) de la LPD[4]. En outre, le COC a également une mission d'avis d'initiative, prévue à l'article 236 §2 de la LPD, et une mission d'information générale du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou de police judiciaire, l'Organe de contrôle émet un avis, soit d'initiative, soit à la demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police concernant toute question relative à la gestion de l'information policière, telle que régie dans la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. L'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel telles que visées aux articles 44/1 à 44/11/13 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 vis-à-vis des services de police, de l'Inspection générale de la police fédérale et de la police locale (ci-après l'« AIG »), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après « BELPIU »), telle que visée dans le Chapitre 7 de la loi du 25 décembre 2016.[6]

---

de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la « Directive Police et Justice » ou *« Law Enforcement Directive »*).

[3] Article 4 §2, quatrième alinéa de la Loi organique APD.

[4] Article 71 §1er, troisième alinéa de la LPD.

[5] Article 59 §1er, 2e alinéa et article 236 §2 de la LPD.

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.

4. Enfin, 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.

II. Objet de la demande

5. Le COC a déjà rendu récemment un avis sur la thématique de la proposition de loi à la demande du ministre de la Sécurité et de l'Intérieur. Le Conseil des Ministres avait en effet décidé en sa séance du 29 mars 2019, concernant un *avant-projet de loi relative à l'approche administrative communale et portant création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics* (point 23 de l'ordre du jour), de soumettre pour avis le projet précité notamment à l'Autorité de protection des données (ci-après 'l'APD'), ce qui a donc été fait le 16 mai 2019 par le ministre de la Sécurité et de l'Intérieur. Le texte a ensuite été transmis le 17 mai 2019 par l'APD à l'Organe de contrôle afin de vérifier, vu certaines de ses dispositions, si l'Organe de contrôle ne devait pas émettre lui aussi un avis au sujet de l'avant-projet de loi susmentionné.

Le COC a effectivement émis un avis sur le texte précité le 17 juin 2019 (voir l'avis DA190013 du 17 juin 2019, https://www.organedecontrole.be/files/DA190013-FR.PDF). Le COC constate toutefois que la proposition de loi qui lui est à présent soumise ne comporte aucune référence à l'avis susmentionné, de sorte qu'il n'est pas clairement établi si les auteurs de l'actuelle proposition de loi ont tenu compte de l'avis du COC, et le cas échéant dans quelle mesure (contrairement à l'avis n° 63.791/2/V du 6 août 2018 du Conseil d'État et aux avis n° 133/2019 du 3 juillet 2019 et 75/2018 du 5 septembre 2018 de l'Autorité de protection des données sur le même sujet).

Le COC insiste auprès du parlement en général et du demandeur en particulier pour que l'avis de l'Organe de contrôle soit toujours repris dans les documents parlementaires, ce qui est régulièrement omis.

6. Étant donné que la proposition de loi qui est à présent soumise présente de nombreuses similitudes avec le texte précédent, et comporte même souvent des dispositions identiques, on peut dans une large mesure renvoyer à l'avis précité émis en juin 2019 par le COC. Pour la simplicité et la lisibilité du présent avis, les remarques formulées à l'époque seront toutefois, dans la mesure où elles sont encore pertinentes, reprises une nouvelle fois afin d'éviter que le législateur ne doive tenir compte de deux avis.

Pour le cadre général, le contexte et les objectifs de la présente proposition de loi, le COC renvoie enfin aux avis suivants de l'APD :

- avis n° 133/2019 du 3 juillet 2019 concernant un avant-projet de loi relative à l'approche administrative communale et portant création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics ;
- avis n° 75/2018 du 5 septembre 2018 concernant une version antérieure (la première) du projet[7] introduit par le ministre de la Sécurité et de l'Intérieur de l'époque, Jan Jambon.

III. Discussion

7. Dans le présent avis, le COC limite son examen aux articles qui concernent directement ou indirectement les traitements policiers de données à caractère personnel repris dans la proposition de loi ou ayant (pouvant avoir) directement ou indirectement une influence sur le fonctionnement de la police intégrée dans le cadre plus large de la gestion de l'information policière.

8. En l'occurrence, il s'agit tout d'abord de l'article 8 de la proposition de loi qui fait partie de la Section 3 (« *La rédaction de l'avis* ») du Chapitre 3 (« *Les missions et le fonctionnement de la DEIPP* ») du Titre 2 (« *Création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics* »). Mais d'autres articles ont également leur importance (directe ou indirecte). Ainsi, le présent avis concerne également les articles 2, 10, 11, 12, 16, 18, 19 et 20. Dans le présent avis, le COC suit la chronologie de la proposition de loi.

8. Les missions de la DEIPP sont définies à l'article 6 comme étant la fourniture d'avis non contraignants à une « *administration requérante* » (une autorité fédérale, régionale ou communale) quant à l'intégrité d'une personne physique ou d'une personne morale chargée en droit ou en fait d'une exploitation, et ce à des fins de prévention de la criminalité grave et organisée. La DEIPP réalisera donc concrètement une enquête d'intégrité sur demande concernant les personnes physiques ou morales précitées qui souhaitent entrer en considération pour remporter un marché public, une concession ou une subvention déterminé(e) (voir l'article 3), ou en présence de signaux susceptibles de contraindre une administration locale de fermer un établissement.

La proposition de loi ne fournit cependant pas de définition d'une « *enquête d'intégrité* ». Il est toutefois possible de déterminer sur la base des projets d'articles 119*ter* et 119*quater* en quoi consiste une telle enquête, quelles sources peuvent être consultées et qui en est chargé. Il n'en demeure pas moins qu'une définition de ce que l'on entend exactement par une « *enquête d'intégrité* » serait la bienvenue. Le Code d'instruction criminelle fournit lui aussi une définition d'une 'information' (article 28bis du Code d'instruction criminelle) et d'une 'instruction' (article 55 du Code d'instruction criminelle). Une enquête d'intégrité est-elle identique à l'« *enquête de moralité* » classique ? À la

[7] Avis n° 75/2018 du 5 septembre 2018 de l'APD concernant un avant-projet de loi relatif à l'approche administrative communale, https://autoriteprotectiondonnees.be/publications/avis-n-75-2018.pdf.

lecture de la proposition de loi, une enquête d'intégrité semble en tout cas plus limitée qu'une enquête de moralité.

Cette enquête d'intégrité a pour but de vérifier si, dans le chef de la personne physique ou de la personne morale chargée en droit ou en fait de l'exploitation et en faisant l'objet :

- il est question d'un risque sérieux qu'il soit recouru à l'exploitation pour utiliser les avantages (financiers) provenant d'infractions déjà commises pour commettre (à l'avenir) des infractions ;
- il existe des indications sérieuses que des infractions ont été commises pour permettre l'exploitation.

Les infractions (ou, pour citer la proposition de loi, les « *faits punissables* ») dont il s'agit sont ensuite énumérés de manière limitative (tant dans le projet d'article 2 que dans le projet d'article 119*ter* §6, 4e alinéa). La proposition de loi a en tout cas le mérite de ne plus retenir la référence à des termes comme « *le fait (ou les indices de fait), par le demandeur ou le candidat, de s'associer pour commettre, de tenter de commettre, d'aider ou d'inciter quelqu'un à commettre ou le conseiller à cet effet, ou de faciliter l'exécution d'un ou de plusieurs faits punissables* », tels qu'ils figuraient dans la version antérieure approuvée par le Conseil des Ministres en sa séance du 29 mars 2019. Ces infractions doivent par contre toujours avoir été commises « *de façon organisée* » (projet d'article 2 et projet d'article 119*ter* §6, 4e alinéa). Tandis que l'exposé des motifs stipule que la finalité de l'enquête d'intégrité vise à prévenir les « *infractions graves et organisées* » et précise que les deux conditions doivent être remplies « *de manière cumulative* »[8], force est de constater que le terme « *graves* » ne figure pas dans la proposition de loi proprement dite. Le texte de la proposition de loi lui-même ne fait donc pas ressortir ces conditions cumulatives. Il convient que l'auteur de la proposition de loi mette le texte en conformité avec l'exposé des motifs.

9. Étant donné que la police intégrée (ci-après la GPI") est définie dans le texte comme un fournisseur de données (à caractère personnel) (projet d'article 8 §1er, 1er tiret) et qu'il apparaîtra rapidement dans la pratique que la GPI sera le principal fournisseur et que les données à caractère personnel devront donc en d'autres termes provenir essentiellement de la GPI, il est primordial que la GPI sache très clairement quelles données sont visées dans la pratique.

Il convient donc de s'interroger dans ce contexte sur la délimitation des matières ou phénomènes qui sont décrits comme « *faits punissables* » et doivent en outre avoir été commis « *d'une façon organisée* ». Des notions telles que fraude fiscale « *grave* » et criminalité environnementale « *grave* » (pour la fraude sociale, la notion de « *grave* » a été supprimée dans cette proposition de loi) restent vagues et volatiles, et constituent des phénomènes criminologiques et non des infractions. Pour le

[8] Doc. Parl., Chambre, 2019-2020, n° 1381, Exposé des motifs, 16 et 17.

COC – et on peut craindre que ce sera également le cas des services de police –, il n'est d'emblée pas clair de savoir ce qu'il y a lieu d'entendre par là et quelles informations/données à caractère personnel peuvent/doivent être communiquées ou non. Si cette notion est déjà utilisée dans le jargon juridique pour la fraude fiscale (et avec un peu de bonne volonté, on peut argumenter qu'il convient d'y conférer la même définition qu'en droit (pénal) fiscal), ce n'est absolument pas le cas pour les autres domaines de criminalité. Dans leurs banques de données policières, les services de police travaillent soit avec des incriminations pénales, soit avec des dénominations/codages propres qui ne correspondent pas d'emblée aux termes utilisés dans le projet et qui sont qualifiés de « *faits punissables* ». Il faut à tout le moins éviter que chaque service de police interprète ces notions différemment pour éviter qu'ils ne transmettent différents types d'informations/de données à caractère personnel, avec également pour conséquence immédiate un traitement inégal des demandeurs. Prenons l'exemple de la « *criminalité environnementale grave* » : les dépôts clandestins en font-ils partie (sous leurs diverses formes) ? À partir de quelle moment la criminalité environnementale est-elle « *grave* » ?

L'Organe de contrôle constate également que la « *criminalité grave alimentaire et dans le secteur des médicaments* » a disparu dans la présente proposition de loi alors qu'il y était fait référence dans les versions antérieures. Pourtant, tant l'Agence fédérale pour la Sécurité de la Chaîne alimentaire (AFSCA) que l'Agence fédérale des médicaments et des produits de santé (AFMPS) peuvent être consultées par la DEIPP concernant les infractions constatées relevant de leur compétence (projet d'article 8 §1er, 9e et 10e tirets), ce qui est étrange étant donné que ces infractions ne comptent plus parmi les « *faits punissables* » pouvant être pris en considération. Il convient que l'auteur de la proposition de loi apporte de la clarté à ce sujet.

10. En outre, ces faits punissables doivent aussi être commis « *d'une façon organisée* ». Ici non plus, on ne donne aucune définition. L'exposé des motifs se borne à indiquer que le terme « *organisé* » doit s'entendre dans son « *acception habituelle* ». Mais quelle est l'« *acception habituelle* » ? L'exposé des motifs précise en tout cas que cette notion ne peut pas être comprise au sens d'« *organisation criminelle* » comme prévu dans le Code pénal (article 324bis du Code pénal). En prévoyant la condition que les faits punissables doivent être commis de façon « *organisée* », on en vient aussi à l'interprétation qu'il peut donc également s'agir de 'criminalité organisée commise d'une façon organisée …' (voir le projet d'article 2, 3e tiret). Tout cela reste donc plutôt obscur.

Il convient d'ailleurs de remarquer qu'en vertu du droit belge, certains de ces « *faits punissables* » ne sont pas du tout des « *infractions* » (bien que ce terme soit utilisé dans le projet d'article 2, 1er alinéa) au sens juridique du terme (et ceux-ci répondent donc à une description de délit avec des éléments constitutifs clairs).

La comparaison avec la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux, dont la liste actuelle des phénomènes criminologiques a été copiée (voir l'article 4, 23° – et non 13°

comme indiqué erronément dans l'exposé des motifs[9]) est quelque peu boiteuse. Les entités soumises à la loi relative à la prévention du blanchiment de capitaux sont investies d'une obligation de dénonciation à la CTIF en ce qui concerne ces phénomènes. La CTIF a alors le choix de communiquer ou non ces informations au ministère public compétent, qui peut ensuite éventuellement ouvrir une information ou requérir une instruction, laquelle peut par la suite être classée sans suite ou donner lieu à une certaine suite pénale. La CTIF ne peut toutefois pas exercer de pouvoirs de contrainte. Elle ne fait que recevoir et analyser les informations communiquées. Dans le cas qui nous occupe, par contre, une implication prétendue dans l'un des « *faits punissables* » précités induit la reprise dans l'enquête d'intégrité ou l'avis de la DEIPP, ce qui peut directement donner lieu à une décision administrative (refus de l'attribution d'une subvention, d'une concession ou d'une adjudication), une sanction (suspension ou abrogation d'un permis) ou une mesure administrative (fermeture d'un établissement), qui a donc un impact immédiat sur la situation juridique de la personne concernée.

11. Il convient de signaler que la condition du « *caractère organisé* » des faits punissables rend particulièrement fastidieuse, pour la GPI, la sélection des données à caractère personnel et des informations entrant en ligne de compte pour une communication. Une simple consultation de la BNG ou des banques de données de base ne suffira pas. Il faudra consulter les procès-verbaux, éventuellement se mettre en rapport avec le parquet pour savoir si une qualification initiale est encore correcte ou pour savoir s'il est question d'un « *caractère organisé* », ou pour savoir tout simplement s'il existe des charges ou a fortiori des preuves (le dossier a-t-il été classé sans suite, si oui pourquoi, y a-t-il eu un renvoi ou un non-lieu, etc.). Ce qui semble organisé à un premier stade d'une enquête peut par la suite se révéler ne pas l'être, ou inversement. Toute une série de « faits punissables » prévus dans la proposition de loi ne présenteront même en principe ou généralement aucun caractère organisé, comme l'escroquerie, l'abus de confiance, la fraude sociale, etc. Mais pour chacun de ces phénomènes, il faudra de toute façon évaluer le caractère organisé. La présente proposition de loi aura donc pour la GPI un impact manifeste en termes de capacité, d'autant que des délais contraignants et courts sont prévus.

12. Le droit au respect de la vie privée tel qu'il est garanti dans la Constitution (article 22) et dans les dispositions pertinentes des conventions (article 8 de la CEDH, articles 7 et 8 et 52, alinéa 1er de la Charte des droits fondamentaux de l'Union européenne) a pour objectif essentiel de protéger les personnes contre les ingérences dans leur vie privée. Ce droit a une large portée et inclut notamment la protection des données à caractère personnel et des informations personnelles[10]. Ce droit au respect de la vie privée n'est pas absolu. Les dispositions évoquées de la Constitution et de la Convention n'excluent pas une ingérence d'une autorité publique dans le droit au respect de la vie privée, mais exigent qu'elle soit prescrite dans une disposition légale suffisamment précise qui répond à un besoin

[9] Doc. Parl., Chambre, 2019-2020, n° 1381, Exposé des motifs, 17.

[10] Voir notamment l'arrêt n° 27/2020 du 20 février 2020 de la Cour constitutionnelle, considérant B.6.4.

social impérieux au sein d'une société démocratique et qui est proportionnelle à la finalité licite poursuivie[11]. Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence dans le droit au respect de la vie privée[12].

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la CEDH implique que sa formulation soit assez précise pour que chacun puisse – en s'entourant au besoin de conseils éclairés – prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé[13]. La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention[14].

13. Pour toutes les raisons qui précèdent, l'Organe de contrôle ne comprend pas pourquoi la proposition ne prévoit pas une liste immuable des infractions (autrement dit, de véritables qualifications pénales) – l'article 90*ter* du Code d'instruction criminelle constituant à cet égard l'exemple évident –, ce qui permettrait de supprimer par la même occasion la notion ou condition de caractère « *organisé* ». Il revient à l'auteur de la proposition de loi de faire au besoin un choix dans cette liste et/ou d'y ajouter d'autres infractions. L'exposé des motifs n'évoque d'ailleurs pas uniquement la criminalité organisée comme finalité : « *Outre l'aspect de l'approche administrative se pose également la question de l'intégrité, à savoir comment éviter que les pouvoirs locaux facilitent, sans le vouloir, la criminalité de droit commun[15] ou la criminalité organisée (…)* »[16].

Une définition claire des infractions augmente dans une large mesure la sécurité juridique. En plus d'offrir davantage de clarté au sujet de droit, elle est aussi pour la GPI plus aisée à utiliser qu'une liste de phénomènes criminologiques. Les infractions figurant sur cette liste sont par nature déjà graves (vu qu'il est uniquement possible, pour ces infractions, d'intercepter, prendre connaissance, explorer et enregistrer des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci) et semblent donc répondre aux finalités de la proposition de loi selon lesquelles il doit s'agir de « *criminalité grave et organisée* », et surtout conférer à l'administration (locale) une position défendable en évitant que des moyens illégaux ne soient injectés dans l'économie régulière ou que les pouvoirs publics ne facilitent inconsciemment cette économie

---

[11] Ibidem, considérant B.7.7 ; voir aussi l'arrêt n° 108/2016 du 14 juillet 2016 de la Cour constitutionnelle, considérant B.10.

[12] Arrêt n° 108/2016 du 14 juillet 2016 de la Cour constitutionnelle, considérant B.11.2 ; soulignement propre.

[13] Arrêt n° 108/2016 du 14 juillet 2016 de la Cour constitutionnelle, considérant B.11.2 avec référence à la CEDH, Grande Chambre, 4 mai 2000, *Rotaru* c. Roumanie, §55 ; Grande Chambre, 17 février 2004, *Maestri* c. Italie, §30).

[14] Arrêt n° 108/2016 du 14 juillet 2016 de la Cour constitutionnelle, considérant B.11.2 avec référence à la CEDH, Grande Chambre, 12 juin 2014, *Fernández Martínez* c. Espagne, §117.

[15] Soulignement propre.

[16] Doc. Parl., Chambre, 2019-2020, n° 1381, Exposé des motifs, 5.

clandestine. Cette liste présente en outre comme avantage d'éviter toutes sortes de contestations et de discussions quant à l'évaluation du caractère « *organisé* » ou non, et de moins surcharger la GPI (et le parquet) en n'imposant pas une enquête détaillée, au niveau du dossier, des données à caractère personnel et informations disponibles.

14. Les termes utilisés (« *infractions* ») impliquent qu'il ne peut pas être question de la communication (voir plus loin), par la GPI à la DEIPP ou au bourgmestre, d'informations de police administrative telles que visées à l'article 44/5 §1er [17] de la LFP et se trouvant dans la BNG, les banques de données de base ou les banques de données particulières. Cela ressort également de plusieurs autres articles de la proposition de loi qui ne prennent en compte que les informations concernant des « *faits punissables* » faisant l'objet de l'avis de la DEIPP ou de l'enquête d'intégrité menée par le bourgmestre (voir le projet d'article 119*ter* §6). Le projet d'article 119*quater* §2, e) limite lui aussi le traitement de données à caractère personnel notamment aux données financières, administratives et aux données en matière judiciaire (excluant donc les données de police administrative). Cette interprétation est confirmée par l'exposé des motifs, qui stipule : « *Il convient de souligner que le traitement de la catégorie de données à caractère personnel visées au §2, e), concerne uniquement les données qui ont trait aux faits punissables énumérés à l'article 18 §6, alinéa 4, de la présente proposition.* »[18].

En ce sens, il est recommandé d'éliminer toute confusion à ce sujet dans le chef de la GPI et d'insérer à l'article 8 §1er, 1er tiret le terme « *judiciaires* » après le terme « *données* ».

15. L'article 8 §1er énumère les services qui peuvent communiquer des informations/données à caractère personnel à la requête de la DEIPP. Il est clair que la DEIPP peut uniquement « *requérir* » – et non imposer – la communication d'informations/données à caractère personnel auprès de ces services. La GPI est mentionnée comme étant l'un des 10 services auxquels une telle requête peut être adressée. La 2e phrase du 2e alinéa est formulée comme suit : « *La communication, l'utilisation et le traitement de ces données se font conformément à la législation qui s'applique pour le service concerné et ne peuvent porter atteinte à l'exercice de l'enquête administrative.* ». Le premier élément de phrase est clair et érige un principe important qui doit en tout temps être pris en compte (également par la GPI).

Le dernier élément de phrase (« *et ne peuvent porter atteinte à l'exercice de l'enquête administrative* ») – qui est répété dans des termes identiques pour l'enquête d'intégrité dans le projet d'article 119*quater* §1er, 4e alinéa – est par contre très problématique. La GPI doit (en concertation avec le parquet, voir plus loin) **toujours** avoir le pouvoir d'opportunité de ne pas communiquer – ou pas intégralement – certaines données, même si cette non-communication entrave l'exercice de

[17] Les données à caractère personnel qui sont traitées à des fins de police administrative dans les banques de données visées à l'article 44/2 §1er, deuxième alinéa, 1° et 2°.

[18] Doc. Parl., Chambre, 2019-2020, n° 1381, Exposé des motifs, 41.

l'enquête administrative ou de l'enquête d'intégrité. Cet élément de phrase est d'ailleurs nouveau par rapport à la version approuvée par le Conseil des Ministres et remplace l'élément de phrase qui stipulait à l'époque qu'« *en tout état de cause, le service interrogé par la DEIPP est autorisé à refuser de fournir les informations demandées par la DEIPP s'il a argumenté la décision de façon suffisante et pertinente* ». À propos de ce passage également, l'Organe de contrôle avait à l'époque déjà fait remarquer que la condition selon laquelle le refus de communiquer entièrement ou partiellement des données à la DEIPP doit être « *argumenté de manière suffisante et pertinente* » n'était pas acceptable pour plusieurs raisons, qui s'appliquent aussi actuellement à l'élément de phrase venu remplacer ce passage (« *et ne peuvent porter atteinte à l'exercice de l'enquête administrative* ») :
- Tout d'abord, la question se pose de savoir qui effectuera l'évaluation du caractère suffisant et pertinent. La DEIPP ne peut pas évaluer si la communication ou non de certaines données porte atteinte à l'exercice de l'enquête administrative ou de l'enquête d'intégrité étant donné qu'elle n'est pas au courant des données en possession de la GPI.
- En ce qui concerne la communication (l'utilisation et le traitement) d'informations judiciaires, cette évaluation est effectuée conformément à la législation qui s'applique pour le service concerné (voir le projet d'article 8 §1er, 2e alinéa et d'article 119*quater* §1er, 4e alinéa). Conformément à la réglementation actuelle, une communication ne peut donc avoir lieu qu'après une évaluation effectuée par le MP ou par la police sous l'autorité du MP qui a la direction et le contrôle des enquêtes en matière pénale. Si la GPI – sous l'autorité du magistrat compétent – ne souhaite pas communiquer des informations/données à caractère personnel (ou certaines d'entre elles), on peut et doit supposer qu'il y a de bonnes raisons à cela : ne pas (encore) vouloir divulguer la phase secrète de l'enquête (pour par exemple ne pas vider de leur sens certaines méthodes de recherche), vouloir protéger certaines sources, un ordre en ce sens du MP, etc. Le but ne peut pas être que les services de police qui fournissent des informations aient à se justifier vis-à-vis de la DEIPP ou du bourgmestre lorsque cette dernière ou ce dernier estime qu'il « *a été porté atteinte* » à l'exercice de l'enquête administrative ou de l'enquête d'intégrité.

L'élément de phrase « … *et ne peuvent porter atteinte à l'exercice de l'enquête administrative* » doit dès lors être supprimé.

16. Une question qui se pose dans la foulée est de savoir si la GPI peut transmettre de manière autonome ces informations/données à caractère personnel en matière judiciaire. Cela ne semble pas être le cas étant donné que « *la communication, l'utilisation et le traitement de ces données se font conformément à la législation qui s'applique pour le service concerné* » (voir le projet d'article 8 §1er, 2e alinéa et d'article 119*quater* §1er, 4e alinéa) et qu'une communication autonome de données judiciaires par la police n'est pas autorisée selon le droit en vigueur.
On peut faire référence aux articles 21*bis* du Code d'instruction criminelle et 1380 du Code judiciaire qui confère au MP compétent le monopole pour la communication des informations judiciaires (comme c'est le cas de longue date). Cet accord préalable peut être soit ponctuel (donc par dossier ou au cas

par cas), soit structurel (via une circulaire par exemple du Collège du ministère public/Collège des procureurs généraux).

17. Le COC fait remarquer que l'arrêté royal délibéré en Conseil des ministres (voir le projet d'article 8 §1er, 3e alinéa) qui fixera les modalités de la nature des données, la demande et la communication des données, y compris la désignation d'un point de contact, si aucun membre du personnel n'était détaché, doit être soumis à l'avis de l'Organe de contrôle en vertu de l'article 59 §1er, 2e alinéa de la LPD.

L'Organe de contrôle rappelle toutefois à cet égard à nouveau (voir plus haut au point 12) qu'en vertu de l'article 8 de la CEDH et de l'article 22 de la Constitution, toute ingérence d'une autorité publique dans le droit au respect de la vie privée doit être prescrite dans une « *disposition légale suffisamment précise* » qui répond à un besoin social impérieux et qui est proportionnelle à la finalité poursuivie. Une telle disposition légale précise doit définir les éléments essentiels des traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique[19]. Dans ce cadre, il s'agit au moins :

a) des finalités déterminées, explicites et légitimes ;
b) des (catégories de) données à caractère personnel qui sont pertinentes et non excessives ;
c) du délai de conservation maximal des données à caractère personnel enregistrées ;
d) de la désignation du responsable du traitement.

La question est de savoir si la condition reprise sous le point b) est suffisamment régie. Le COC est en tout cas d'avis qu'on ne sait pas clairement, en ce qui concerne la condition reprise au point b), quelles catégories d'informations peuvent être communiquées :

- uniquement des informations relatives à des faits concrets ou également ce qu'on appelle des « informations douces » ; lorsqu'on relit les critères pouvant conduire à la non-délivrance, à la suspension ou à l'abrogation d'un permis ou à la fermeture d'un établissement sur la base de l'enquête d'intégrité qui a été menée, on doit conclure que le but est peut-être de prendre en considération n'importe quel type d'informations (aussi les faits non concrets, aussi des informations non validées, etc.) (voir le projet d'article 119*ter* §6 de la NLC qui parle de « *présomptions raisonnables* », « *que l'établissement sera exploité* », « *le rapport entre l'exploitant et les faits punissables* », « *exercer de façon indirecte des fonctions de direction* », « *un tiers exerçant une influence commerciale sur l'exploitant* », qui sont tous des termes (pouvant être) relatifs à des faits, des allégations, des circonstances ou des informations doux (douces) et/ou non validé(e)s) ;

[19] Voir DEGRAVE, E., « L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle », Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (voir par ex. : CEDH, arrêt Rotaru c. Roumanie, 4 mai 2000). Voir également notamment les arrêts suivants de la Cour constitutionnelle : l'arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'arrêt n° 29/2018 du 15 mars 2018 (p. 26).

- des informations provenant uniquement de sources nationales ou également de sources internationales (banques de donnée d'Europol, données d'Interpol, etc.) ;
- des informations sous embargo (soit un embargo légal imposé par le MP, soit un code d'utilisateur limité comme le prévoit la circulaire Ministérielle MFO-3) ;
- quid de toutes les informations/données à caractère personnel qui ne concernent pas le demandeur ou « *les personnes chargées en droit ou en fait de l'exploitation* » (voir le projet d'article 119*ter* §5 de la NLC), comme des membres de la famille, des amis, des connaissances, des témoins, des victimes, ... Ces données se retrouveront-elles aussi dans le dossier de la DEIPP ou dans le dossier administratif final ? La GPI doit-elle sécuriser ces données avant de les communiquer ? En son article 31, la LPD impose aux services de police, dans la mesure du possible, d'établir une distinction entre les différentes catégories de personnes (auteurs, victimes, témoins, dénonciateurs, ...). L'article 10 §2 de la proposition de loi dispose que l'avis de la DEIPP ne peut pas mentionner des données qui pourraient notamment porter préjudice à la protection de la vie privée de tiers. Il s'agit d'emblée d'un aspect important mais la question est de savoir si cela prévient tout risque que des données à caractère personnel portant préjudice à la vie privée des tiers susmentionnés se retrouvent dans le dossier de la DEIPP ou dans celui de l'autorité administrative qui prend la décision (dossier de l'enquête d'intégrité). À la lecture de l'article 12 qui contient une description du contenu du dossier de traitement de l'avis, cela ne semble pas être le cas, étant donné que le point 3 mentionne « *les demandes de données conformément à l'article 8 et les données qui ont ainsi été communiquées* (soulignement propre)*, ainsi que le service ou l'autorité qui les ont fournies* » ;
- etc.

18. La désignation des (catégories de) données à caractère personnel qui sont pertinentes et non excessives et qui peuvent être transmises à la DEIPP par les services qui les ont fournies doit donc être régie dans le projet et ne peut pas être traitée dans un arrêté royal (voir également ci-après au point 25). La dénomination prévue à l'article 119*quater* §2, e) – « *les données financières, administratives et les données en matière judiciaire* » – est à ce point générique qu'elle ne semble pas répondre aux exigences d'une disposition légale suffisamment précise que nous évoquions plus haut.

En ce qui concerne la GPI, l'Organe de contrôle plaide au moins pour que les informations devant potentiellement être communiquées par la GPI soient limitées aux informations « dures » (validées), autrement dit aux informations qui ont été consignées dans un procès-verbal. Vu les conséquences potentiellement lourdes pour la personne concernée, il convient d'éviter que des informations douces (non validées) soient également communiquées à la DEIPP ou aux bourgmestres. Permettre tout de même cette communication serait de l'avis du COC disproportionné et confronterait la GPI à des problèmes d'application pratique additionnelles qui engendreraient des problèmes de capacité. Il convient d'ailleurs de faire remarquer à ce sujet que les circulaires applicables du 13 octobre 2017 des procureurs généraux de Gand et d'Anvers relatives à la participation du ministère public à l'approche

administrative de la criminalité et des phénomènes liés à l'insécurité prévoient également qu'il ne soit « *jamais communiqué à l'administration (locale) d'**informations douces** (informations reprises dans un rapport d'information (RIR) ou un rapport confidentiel) ni **d'informations sous embargo** ou s'assortissant d'un **code d'utilisateur limité*** »[20]. L'Organe de contrôle plaide pour que cette règle claire soit également reprise dans la proposition de loi en ce qui concerne la GPI.

19. En outre, l'attention de l'auteur de la proposition de loi est attirée sur l'article 44/11/9 §2 de la LFP, récemment modifié par la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière[21], qui est actuellement libellé comme suit :
« §2. Selon les modalités déterminées par les directives des ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, elles (les données à caractère personnel et informations policières, NDLR) *peuvent également être communiquées aux autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique lorsque ceux-ci en ont besoin pour l'exécution de leurs missions légales. La liste de ces autorités, organes ou organismes est arrêtée par les ministres de l'Intérieur et de la Justice sur la base d'une proposition du Comité information et ICT visé à l'article 8sexies de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux. L'avis de l'Organe de contrôle de l'information policière concernant cette proposition est sollicité.* (soulignement propre) »

La première question qui se pose est de savoir quel est le lien entre le projet d'article 8 §1er, 1er tiret et le projet d'article 119*quater* §1er, e) de la NLC, d'une part, et l'article 44/11/9 §2 modifié de la LFP, d'autre part. La DEIPP est incontestablement une autorité publique belge, un organe ou organisme public ou d'intérêt public mais la question est de savoir si elle a aussi des « *missions légales de sécurité publique* ». Cela ne semble pas si évident, étant donné que la DEIPP a uniquement une mission d'avis non contraignant. En outre, la DEIPP doit être reprise dans la liste des organismes par les deux ministres de tutelle sur proposition du nouveau 'Comité Information et ICT' visé à l'article 8*sexies* de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (LPI), proposition sur laquelle l'Organe de contrôle doit également rendre un avis propre.

Quel est le lien entre ce cadre légal relatif à la communication d'informations policières à des *Law Enforcement Agencies* tierces de l'article 44/11/,9 §2 de la LFP et la présente proposition de loi, en ce qui concerne la DEIPP ? La présente proposition de loi doit-elle être perçue comme une dérogation aux règles de la LFP ? L'Organe de contrôle lit également dans le projet d'article 119*quater* §1er, 4e

[20] Circulaire 11/2017 du 13 octobre 2017 du procureur général de Gand relative à la participation du ministère public à l'approche administrative de la criminalité et des phénomènes liés à l'insécurité, point 25, *non publiée* ; Circulaire 10/2017 du 13 octobre 2017 du procureur général d'Anvers relative à la participation du ministère public à l'approche administrative de la criminalité et des phénomènes liés à l'insécurité, point 25, *non publiée*.

[21] *Moniteur belge* du 19 juin 2019 ; voir aussi *Doc. Parl.*, *Chambre*, 2018-2019, n° DOC 54, 3697/001 à 007 inclus.

alinéa que « *la communication, l'utilisation et le traitement de ces données se font conformément à la législation qui s'applique au service concerné* ». En d'autres termes, les règles de la LFP semblent donc primer, ce qui signifie qu'une communication de données de la GPI à la DEIPP n'est pas possible aussi longtemps que l'article 44/11/9 §2 de la LFP n'aura pas été correctement mis en œuvre.

L'auteur doit apporter de la clarté à ce sujet.

20. L'article 11, *in fine*, prévoit que la DEIPP tient des fichiers de journalisation qui sont conservés pendant 10 ans (dans les versions précédentes, il était question de 3 ans). Un délai similaire est prévu pour les traitements de données à caractère personnel réalisés par le bourgmestre (les services du bourgmestre) lors de l'exécution de ce qu'on appelle l'enquête d'intégrité (voir le projet d'article 119*quater* §4, 2e alinéa de la NLC).

Il est également essentiel pour les services de police (et tous les autres services fournisseurs d'informations) que soient tenus des fichiers de journalisation des traitements d'informations/de données à caractère personnel provenant des services de police fournisseurs. En cas de violation de la sécurité ou de *data breach*, il est essentiel de pouvoir retracer la source de la violation, a fortiori vu le type de données que la DEIPP reçoit de la police. À cet égard, un délai de 10 ans est acceptable et correspond davantage aux délais de 30, 15 ou 10 ans prévus par la LFP pour les fichiers de journalisation des banques de données policières (article 44/9 §3 et article 44/10 §1er en ce qui concerne la BNG : 30 ans ; article 44/11/2 §8 en ce qui concerne les banques de données de base : 15 ans avec une possibilité de prolongation jusqu'à 30 ans ; et article 44/11/3 §4 en ce qui concerne les banques de données particulières : 10 ans avec possibilité de prolongation jusqu'à 30 ans). On peut partir du principe que la plupart des informations qui seront transmises de la police vers la DEIPP ou le bourgmestre (les services du bourgmestre) proviendront de la BNG ou des banques de données de base.

21. Il convient d'accorder l'attention requise au fait que les données ne peuvent être conservées que pendant une durée limitée et que ces délais ne sont pas uniformes et ne correspondent pas non plus à ceux stipulés pour la journalisation. Le dossier de traitement de l'avis de la DEIPP est archivé immédiatement après la transmission de l'avis de la DEIPP au demandeur ; le dossier archivé doit être détruit au bout de 1 an, à l'exception de l'avis proprement dit qui est détruit après 3 ans (projet d'article 12). Les données du fichier communal des enquêtes d'intégrité sont quant à elles conservées pendant 5 ans à compter de la clôture de l'enquête d'intégrité (projet d'article 119*quinquies* §2 de la NLC, *in fine*), après quoi elles doivent être détruites ou anonymisées, à l'exception des données sur lesquelles se fonde la décision de refus, de suspension ou d'abrogation d'un permis ou de fermeture d'un établissement accessible au public, lesquelles doivent être détruites immédiatement après que la décision susmentionnée a acquis un caractère définitif. Il semble indiqué de prévoir les mêmes délais

de conservation et le même régime pour la DEIPP et pour la commune. En tout état de cause, la durée de la période de journalisation excède donc largement le délai de conservation des données.

22. L'article 12 comprend une énumération du contenu du dossier d'avis de la DEIPP. La première question fondamentale qui se pose est de savoir si ce dossier peut être accessible pour le demandeur ou une autre partie intéressée. Il est évidemment essentiel que les services de police le sachent. D'après le 2e alinéa du §1er, ce dossier « *de traitement de l'avis* (…) *n'est disponible ou ne peut être consulté que par les membres désignés par le directeur de la DEIPP, en fonction de la nécessité d'en prendre connaissance* ». Il faut donc partir du principe que la loi sur la publicité de l'administration du 11 avril 1994 ne s'applique pas ici ou plutôt que la présente proposition de loi déroge à cette loi. Il semble préférable de reprendre cette exception *expressis verbis* dans la loi proprement dite ou au moins dans l'exposé des motifs. L'alinéa susmentionné est rédigé de manière si affirmative qu'on ne sait pas non plus clairement si la GPI ou le parquet peuvent consulter le dossier précité (au besoin, sous la contrainte). Cette disposition touche-t-elle par exemple aux compétences pénales en matière de saisie de la GPI et du MP ? L'auteur de la proposition de loi est prié de préciser cet aspect. Il semble recommandé d'également déclarer applicable le 2e alinéa du §2 au §1er de manière à ce que non seulement le dossier archivé mais aussi le dossier « vivant » puisse être consulté par les autorités judiciaires (et la GPI) dans le cadre de la détection et de la poursuite d'infractions.

23. Le projet d'article 14 prévoit un régime particulier qui limite les droits de la personne concernée en vertu du droit à la protection des données. Le paragraphe 1er stipule : « *La demande d'exercer les droits visés aux articles 14, 15, 16, 18 et 21 du Règlement (UE) 2016/679, à l'égard des traitements de données à caractère personnel réalisés par la DEIPP et ses fournisseurs d'information visés à l'article 8 §1er, est adressée à l'autorité de protection des données.* ». L'ajout des termes « *et ses fournisseurs d'information* » est nouveau par rapport aux versions antérieures et est problématique. Les informations fournies par la GPI sont en effet soumises au régime élaboré à l'article 14 de la loi sur la protection des données qui s'applique à la DEIPP. Il existe donc une contradiction entre le projet d'article 14 prévu par la présente proposition de loi et l'article 14 de la LPD. Le COC demande donc à ce que les termes « *et ses fournisseurs d'information* » soient supprimés afin d'éliminer l'ineptie ainsi créée.

Les personnes concernées exercent leurs droits uniquement à l'égard des traitements de données effectués par la DEIPP. Seul cet aspect doit être régi dans la présente proposition de loi. Ce projet d'article 14 prévoit à cette fin un système d'accès indirect auprès de l'APD (le COC ne se prononce pas sur l'opportunité de ce choix, mais renvoie à l'avis de l'APD), dans le cadre duquel cette dernière peut uniquement communiquer « *qu'il a été procédé aux vérifications nécessaires* ». Il est toutefois ajouté que l'APD peut communiquer à la personne concernée certaines informations contextuelles (projet d'article 14 §1er, 3e alinéa).

L'exercice des droits d'une personne concernée à l'égard de la GPI est régi par les articles 41 et 42 de la LPD, qui prévoient également un système d'accès indirect auprès du COC. Depuis le 1er septembre 2018, le COC a ainsi déjà traité plus de 500 dossiers. Le COC ne peut toutefois pas fournir d'initiative certaines informations contextuelles (voir l'article 42, 3e et 4e alinéas) étant donné qu'il y a lieu de d'abord encore promulguer un arrêté royal qui devra déterminer les catégories d'informations contextuelles qui peuvent être communiquées. Cet arrêté royal n'a toujours pas été promulgué, de sorte que le COC est tenu depuis le 1er septembre 2018 (date de l'entrée en vigueur de la LPD) de limiter sa communication à l'intention du demandeur/de la personne concernée à l'indication « *qu'il a été procédé aux vérifications nécessaires* », ce qui engendre très souvent une grande frustration dans le chef de la personne concernée.

Le régime projeté ici permettrait toutefois à l'APD de fournir des informations contextuelles provenant initialement de la GPI, alors que le COC ne peut pas fournir d'informations contextuelles à une personne concernée. Il convient évidemment d'éviter cette contradiction. Dès qu'il apparaît que la DEIPP dispose d'informations provenant de la GPI, l'article 14 de la LPD doit être appliqué, ce qui signifie que l'APD s'adresse alors au COC, le tout conformément aux paragraphes 5 et 6. Autrement dit, le projet d'article 14 de la présente proposition de loi court-circuite l'application de l'article 14 de la LPD et risque de donner lieu à des réponses différentes, de la part respectivement de l'APD et du COC (pour autant qu'il s'agisse d'informations policières), à des demandes émanant d'une même personne concernée. Il va de soi que cette situation doit être évitée.

Le projet d'article 119*sexies* §1er tient en revanche correctement compte de l'article 14 (et de l'article 16) de la LPD.

Pour résumer, le COC demande donc d'une part de supprimer dans le premier alinéa du §1er les termes « *et ses fournisseurs d'information* », et d'autre part d'ajouter à ce §1er un alinéa correspondant à l'article 42, 4e alinéa de la LPD : « *Le Roi détermine, après avis de l'autorité de contrôle compétente, les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée, par cette autorité de contrôle.* ».

24. La clause de confidentialité du projet d'article 16 ne peut pas non plus s'appliquer à l'égard des autorités de contrôle. Ainsi, il est clair qu'un membre détaché de la GPI, qui est ainsi devenu membre du personnel de la DEIPP, ne peut ou ne pourrait pas invoquer ce secret dans le cadre d'enquêtes et de contrôles menés par l'Organe de contrôle. Cela s'applique d'ailleurs aux autres autorités de contrôle. Cet article doit donc être amendé comme suit : « *En dehors des cas où ils sont convoqués pour témoigner en droit en matière pénale ou devant une commission d'enquête parlementaire ou à l'égard de l'autorité de contrôle compétente dans le cadre de l'exercice de leurs missions, le directeur, les agents détachés et les magistrats de liaison ainsi que les membres du personnel de la DEIPP sont liés par le secret professionnel et ne peuvent communiquer à aucune personne ou autorité des données*

dont ils ont eu connaissance dans le cadre de l'exercice de leurs compétences, en vertu de la présente loi. Le secret doit être maintenu même lorsqu'ils ont quitté la DEIPP ou ont cessé leur collaboration. ».

Le COC ne comprend par ailleurs pas pourquoi la GPI n'a pas été reprise dans l'exception au devoir de confidentialité du §1er de l'article 16 telle qu'elle est prévue au 1er tiret du §2. Aussi la GPI joue bien évidemment un rôle crucial dans la lutte contre l'extrémisme, le terrorisme et leur financement, de sorte qu'il serait indiqué de prévoir une dénonciation spontanée de la part de la DEIPP à la GPI (ou à un point de contact choisi, par exemple la DGJ/DJSOC[22] de la police fédérale). Il en va de même des demandes émanant des services et adressées à la DEIPP. Là aussi, on peut difficilement comprendre pourquoi la DEIPP est tenue d'accéder à une demande d'informations émanant des services de renseignement, de la CTIF, de l'OCAM et des autorités judiciaires, alors que la GPI ne semble pas pouvoir introduire une telle demande – ou du moins qu'aucune obligation d'y accéder n'a été prévue dans le chef de la DEIPP. À moins que l'on ne veuille faire passer toutes les demandes de la GPI par le parquet ? Pour des raisons d'efficacité et de capacité, cette option semble tout sauf opportune au COC.

25. Le §4 du projet d'article 119*ter* de la NLC dispose que le bourgmestre désigne les membres du personnel chargés de l'enquête d'intégrité qui est prévue. Le projet de §12 prévoit que le Roi « (détermine) *les modalités minimales de l'analyse de risques préalable et les conditions relatives aux membres du personnel chargés de l'enquête d'intégrité* ». Le COC se demande si les membres de la police locale sont aussi visés par cette disposition. Si c'est le but, il est préférable de le préciser explicitement, au moins dans l'exposé des motifs. Il est en effet important que les zones de police sachent qu'elles peuvent être chargées de cette enquête d'intégrité, vu l'impact sur leur capacité opérationnelle, d'autant plus que des délais très courts (en principe 30 jours) sont prévus pour boucler cette enquête (abstraction faite de la possibilité de prolonger ce délai une fois de 30 jours). Cela signifie effectivement que de telles enquêtes d'intégrité devront recevoir la priorité absolue avec toutes les conséquences qui en découlent sur l'exécution des autres missions de police de base par la police locale (comme les missions locales de recherche, le travail de quartier local, etc.). Il appartient à l'auteur de la proposition de loi de reconsidérer ce délai particulièrement strict, qui est de plus un délai de déchéance et non un délai d'ordre, en sachant qu'une telle enquête concerne ou peut également concerner la personne physique ou morale qui sera chargée non seulement en droit mais aussi en fait de l'exploitation. Rien que la recherche de la personne qui sera chargée en fait de l'exploitation peut requérir une enquête approfondie et donc du temps. L'Organe de contrôle estime que le délai prévu de 30 jours n'est pas réaliste et risque de donner lieu à des erreurs, des négligences et des échecs.
Il semble au moins vivement recommandé de faire de ce délai un délai d'ordre.

[22] La Direction centrale de la lutte contre la criminalité grave et organisée de la Direction générale de la police judiciaire.

26. En ce qui concerne le projet d'article 119*quater* §1er, e) de la NLC, l'Organe de contrôle renvoie *mutatis mutandis* à ce qui a été précisé ci-dessus aux points 9 à 18 inclus. Ici non plus, il n'y a pas la moindre précision quant aux catégories de données que la GPI peut transmettre au bourgmestre (aux services du bourgmestre) dans le cadre de l'enquête d'intégrité. En l'occurrence, c'est encore plus problématique car, dans l'hypothèse où aucun avis n'est demandé à la DEIPP, ce qui n'a pas été rendu obligatoire, il n'y a donc aucune intervention d'un *trusted third party* (tiers de confiance), ce qu'est la DEIPP (une qualité qui est également soulignée à plusieurs reprises dans l'exposé des motifs[23]), et toutes les informations policières sensibles possibles de nature judiciaire peuvent directement arriver chez le bourgmestre, sans le moindre filtre. Dans ce cadre, le bourgmestre est le chef de la police locale qui se trouve sous son autorité (articles 11 et 42 de la Loi sur la Police intégrée) de sorte qu'il n'est pas si évident, pour une police locale, de refuser certaines informations au bourgmestre ou de les filtrer.

En ce qui concerne les données judiciaires, il est en outre prévu qu'« *au sein du conseil zonal de sécurité, un protocole est conclu au sujet des enquêtes d'intégrité dans lesquelles des données judiciaires peuvent être utilisées. Ce protocole contient au moins une description du champ d'application matériel et territorial, ainsi que les modalités de communication et d'utilisation des informations* ». Que se passe-t-il si aucun protocole n'est conclu ? Un protocole ou de préférence un accord ne peut en effet pas être forcé. Il semble dès lors que dans cette hypothèse, aucune information judiciaire ou information policière de nature judiciaire ne peut être communiquée, par les services de police non plus. Il appartient à l'auteur de la proposition de loi de distinguer cette hypothèse.

27. Le §2 du projet d'article 119*quater* tente de décrire les catégories de données à caractère personnel qui seront traitées dans le cadre d'une telle enquête d'intégrité. Comme précisé aux points 9 à 18 inclus et au point 25, cela reste toutefois très vague : la catégorie la plus importante, faisant l'objet essentiel de la présente proposition de loi, est en effet le point e), ce qui est défini comme étant « *les données financières, administratives et les données en matière judiciaire pour autant que ces données à caractère personnel émanent des instances visées au paragraphe 1er* ». Peut-être les données de police judiciaire (cf. article 44/5 §3 de la LFP) qui proviennent de la GPI peuvent-elles alors être incluses sous le dénominateur « *données en matière judiciaire* ». Quoi qu'il en soit, cette énumération est si large qu'elle ne répond pas aux normes juridiques fondamentales précitées telles que contenues dans la CEDH, la Charte des droits fondamentaux de l'Union européenne, le RGPD ou la Constitution.

[23] Doc. Parl., Chambre, 2019-2020, n° 1381, Exposé des motifs, 14 : « *La DEIPP constituera ainsi un filtre entre les différentes administrations qui fournissent des informations et celles qui les utilisent.* (…) *Cela permettra de limiter au maximum le risque de traitement illégitime et inapproprié de l'information.* ». Doc. Parl., Chambre, 2019-2020, n° 1381, Exposé des motifs, 18 : « (…) *Une certaine neutralité à l'égard des autorités requérantes s'impose.* ».

28. Le COC souhaite pour terminer attirer l'attention de l'auteur de la proposition de loi sur quelques références croisées dans le texte qui semblent ne pas être correctes, par exemple :
- projet d'article 10 §1er : la référence à l'article 7, premier alinéa doit sans doute être une référence à l'article 7 §1er ;
- projet d'article 11, 3e alinéa, 4° : la référence à l'article 119*quater*, deuxième alinéa n'est pas claire. Le deuxième alinéa de quel paragraphe ? ;
- le chapitre 5 du titre 2 doit être le chapitre 4 et le chapitre 6 doit être le chapitre 5 ;
- projet d'article 119*ter* §1er : la référence à l'« *alinéa 4* » semble ne pas être correcte ; il se pourrait qu'il s'agisse du §6, 4e alinéa ;
- projet d' article 119*ter*, §4, 2e alinéa: les mots "*zijn gehouden*" (version en néerlandais) doivent être supprimés;
- projet d'article 119*quater* §4, 2e alinéa, 4° : la référence à l'article 119*ter* §6, a, b et c n'est pas complète et doit être une référence à l'article 119*ter* §6, 3e alinéa, a), b) et c) ;
- projet d'article 119*sexies* §3, 1er alinéa : la référence « *visées à l'alinéa 1er, c)* » n'est pas claire.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

requiert le demandeur de donner suite aux remarques reprises aux points 9 à 28 inclus ;

demande pour le reste qu'il soit tenu compte des remarques susmentionnées reprises aux autres points ;

Avis approuvé par l'Organe de contrôle de l'information policière le 15 septembre 2020.
Pour l'Organe de contrôle,
Le Président,

(sé.) Philippe ARNOULD