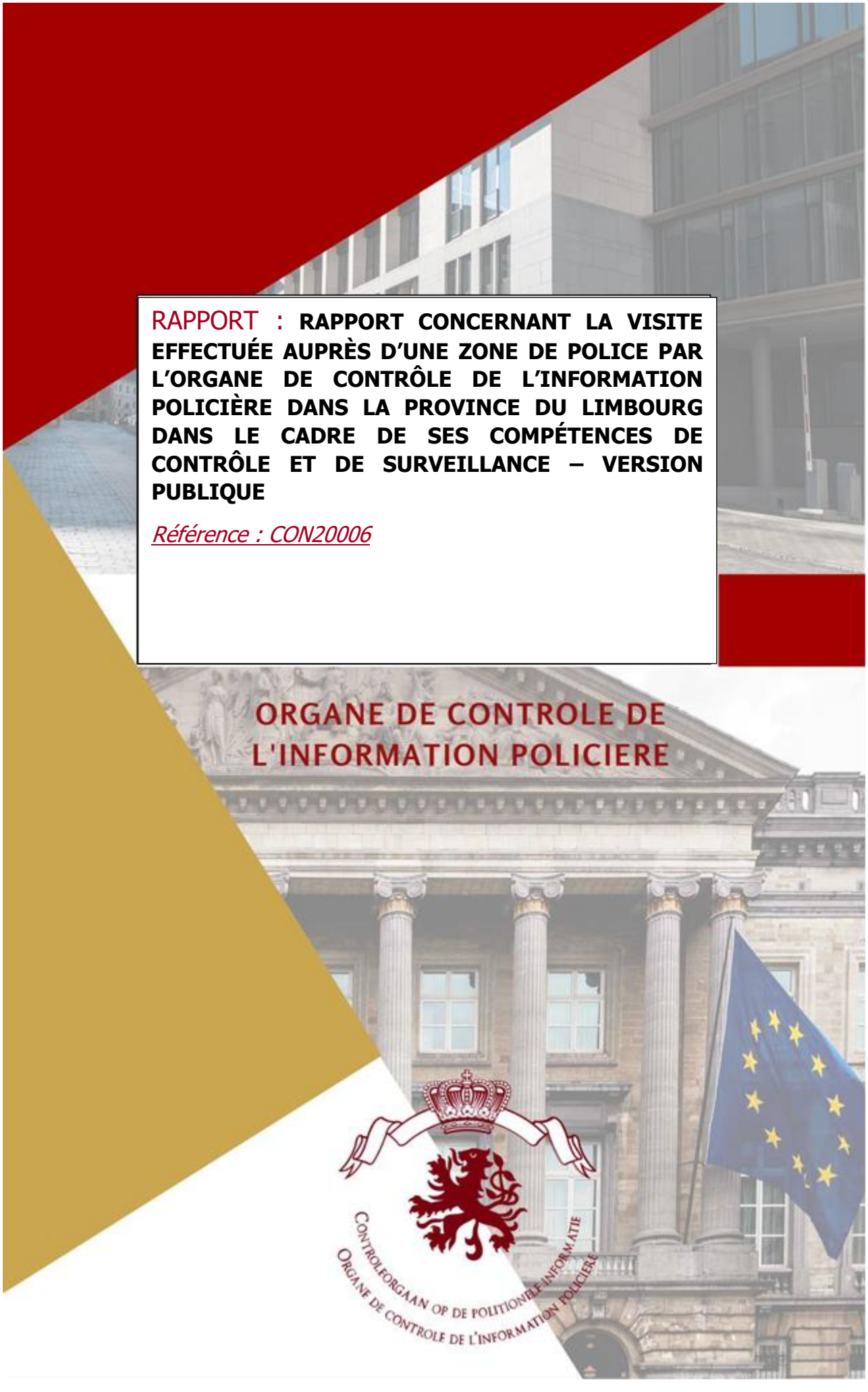

RAPPORT : **RAPPORT CONCERNANT LA VISITE EFFECTUÉE AUPRÈS D'UNE ZONE DE POLICE PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LA PROVINCE DU LIMBOURG DANS LE CADRE DE SES COMPÉTENCES DE CONTRÔLE ET DE SURVEILLANCE – VERSION PUBLIQUE**

Référence : CON20006

TABLE DES MATIÈRES

SYNTHÈSE DE LA VISITE 4
Objet et conception de l'étude 4
Conclusions de l'étude 4
Conclusion – recommandations – mesures correctrices 5
Conclusion 5
Recommandations 6
Mesures correctrices 8
1. INTRODUCTION 9
1.1. Les compétences de l'Organe de Contrôle 9
1.2. Objectifs 10
2. CONCEPTION DE LA VISITE ET MÉTHODOLOGIE 10
2.1. Contexte 10
2.2. Méthodologie 11
3. DISPOSITIONS LÉGALES ET RÉGLEMENTAIRES PERTINENTES 11
3.1. Généralités 11
3.2. Activités de traitement policières et non-policières 12
3.3. Surveillance par caméra et application de la LPD 12
3.3.1. Responsable du traitement 13
3.3.2. Exigences procédurales 13
3.3.3. Délai de conservation des images 14
3.3.4. Banques de données techniques 14
3.3.5. Accès aux images 14
3.3.6. Utilisation visible et non visible de caméras 14
3.3.7. Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou *DPIA*, *Data Protection Impact Assessment*) 15
3.3.8. Registre 15
3.3.9. Journalisation 15
3.4. Gestion fonctionnelle 16
4. CONCLUSIONS DES RECHERCHES ET ANALYSE JURIDIQUE 16
4.1. Traitements policiers 16
4.1.1. L'utilisation de la surveillance par caméra classique et des caméras ANPR : approbation du conseil communal 16
4.1.2. Responsable du traitement pour les caméras *ANPR* fixes 17
4.1.3. Délai de conservation des images et banque de données technique 18
4.1.4. Cellules de police 18
4.1.5. Autres types de surveillance par caméra 28
4.1.6. Accès aux images (identifiant) et connexion (moment, motif de la consultation) 18
4.1.7. Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou *DPIA*, *Data Protection Impact Assessment*) 19
4.1.8. Registre des images des caméras et des activités de traitement 19
4.1.9. La corrélation des images ANPR avec les listes locales 20
4.2. Le traitement de données dans la BNG 21
4.2.1. La gestion fonctionnelle 21
4.2.2. La validation des données (validation centrale) 23
4.3. Banques de données particulières 23
4.4. L'utilisation d'appareils mobiles dans le cadre ou non de missions opérationnelles et l'utilisation d'images caméra à des fins non opérationnelles 24
4.5. Protection des données 25
4.5.1. Le traitement de données biométriques à des fins non opérationnelles 26
4.5.2. Le consentement 26
4.5.3. Intérêt public important 26
4.5.4. Obligations du responsable du traitement (le chef de corps) 27
4.5.5. Le registre des traitements 28

4.6. Le délégué à la protection des données (DPO) 28
4.7. Sécurité des informations 30
4.7.1. Politique et organisation 30
4.7.2. Fichiers de journalisation de propres systèmes ICT (« traçabilité ») 31
4.7.3. Gestion des accès 31
4.7.4. Planification de la continuité 32
5. CONCLUSION – RECOMMANDATIONS – MESURES CORRECTRICES 32

SYNTHÈSE DE LA VISITE[1]

Objet et conception de l'étude

Le 28 octobre 2020, l'Organe de Contrôle a effectué une visite globale dans une zone de police locale dans la province du Limbourg. La visite s'inscrit dans le cadre du Plan stratégique de l'Organe de Contrôle qui prévoit d'effectuer chaque année des visites de plusieurs zones de police et entités de la police fédérale en vue de l'exécution de ses compétences de contrôle et de surveillance. Le contrôle dans la zone de police était une visite spontanée. Elle n'était donc pas la conséquence d'une plainte (individuelle) ou de l'existence d'indices (concrets) du non-respect de la législation et de la réglementation par la police locale visitée.
Le choix s'est porté sur une visite en largeur. Cela signifie que celle-ci portait sur plusieurs thèmes sans s'attarder sur aucun en particulier. En l'occurrence, une attention particulière a été accordée à l'application du cadre juridique en matière de protection des données.

La visite portait abordait cinq thèmes :

1) l'utilisation de caméras ;
2) la gestion des données et informations dans la BNG ;
3) les banques de données particulières ;
4) les systèmes de contrôle du personnel ;
5) la sécurité de l'information : organisation, politique et gestion ICT.

Conclusions de l'étude

La police dispose d'un nombre limité de caméras fixes dirigées sur l'espace public, trois caméras *ANPR* fixes et une caméra *ANPR* mobile. Fait intéressant, la zone de police n'a pas pu donner immédiatement une réponse à la question de l'identité précise du responsable du traitement pour les 2 caméras ANPR fixes à la frontière avec les Pays-Bas. Il ressort toutefois de l'étude que la zone de police est effectivement la responsable du traitement pour ces 2 caméras *ANPR* même si les images ne sont pas conservées par la ZP mais par (la direction d'arrondissement de) la police fédérale. En ce qui concerne les caméras fixes de la police qui surveillent l'espace public et la caméra *ANPR* mobile (utilisation visible de la caméra), le consentement du conseil communal n'a pas été demandé, de sorte que celle-ci n'est pas utilisée conformément à la loi. Le consentement du conseil communal n'a été donné que le 24 novembre 2020, donc après la date de la visite, et transmis à l'Organe de Contrôle le 18 janvier 2021.

Au moment de la visite, l'accès aux images des caméras était basé sur un identifiant (de service) général, ce qui n'est pas conforme aux obligations légales. Un accès individualisable aux images des caméras *(ANPR)* n'est pas utilisé et aucun contrôle du fichier de journalisation des images de la caméra *ANPR* mobile ne peut être effectué, ce qui est pourtant obligatoire légalement. La zone de police ne disposait pas non plus d'une gestion des accès et des utilisateurs élaborée (concrètement) en matière d'utilisation des caméras. La même constatation vaut pour la constitution de la banque de données technique locale pour les images *ANPR* qui sont enregistrées sur un ordinateur portable par la ZP, ce qui en fait une « banque de données technique ». Préalablement à l'utilisation de l'*ANPR* mobile, une *DPIA* (analyse d'impact en matière de protection des données) n'a pas été effectuée et l'avis du *DPO* n'a pas été obtenu avant la constitution d'une banque de données technique locale. La zone de police ne disposait pas non plus d'un registre consignant l'utilisation des caméras.

Les services de police traitent aussi des données à caractère personnel à des fins non policières. Dans ce cas, le RGPD est d'application, en plus de la LPD[2]. À cet égard, la ZP utilise aussi des images de caméra policières ou des données numériques en vue du traitement des plaintes ou du contrôle du respect des conditions de travail (en ce qui concerne l'utilisation des infrastructures de réseau mises à disposition par la ZP). Sur ce dernier point, la procédure appliquée par la ZP est le reflet ou l'application analogue des principes de la convention collective de travail (CCT) n° 81 relatifs au

[1] Une version publique d'un rapport signifie que celle-ci ne contient pas nécessairement tous les éléments figurant dans le rapport de base qui est adressé à l'un des destinataires. Certains éléments ou passages ont été supprimés ou anonymisés. Il peut y avoir diverses raisons à cet effet, tant des raisons de nature légale que des motifs d'opportunité : la non-divulgation de techniques ou tactiques policières, le secret de l'instruction, le secret professionnel, le fait qu'il ait été remédié à un manquement entre-temps, etc.
[2] La loi du 30 juillet 2018 « *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ».

contrôle de l'utilisation d'Internet. Pour le COC, cette attitude de base est tout bonnement une meilleure pratique. En dépit du caractère exceptionnel de ces contrôles, cela ne doit pas empêcher la ZP d'établir en la matière une *politique* qui définit la procédure, les conséquences et les droits du personnel de la police. Il en va de même pour l'utilisation d'images de caméras policières pour le contrôle du respect des conditions de travail du personnel.

Un très bon fonctionnement a pu être constaté sur le plan de la gestion des informations. Un contrôle de qualité des données a été effectué préalablement au flux destiné à la Banque de données nationale générale (ci-après « BNG »). L'option 32[3] est exécutée par la Zone de Police HANO sur le plan de la corrélation des images ANPR avec les listes nationales. Cela implique toutefois que l'utilisation des *blacklists* ou listes nationales n'est pas journalisée pour la ZP. Par conséquent, un transfert intervient d'une manière qui ne doit pas encore être expliquée par la ZP au moment de la rédaction de ce rapport.

La ZP utilise des banques de données particulières qui sont enregistrées dans le registre des traitements. Toutefois, certaines de ces banques de données peuvent difficilement être considérées comme des banques de données particulières.

La zone de police a une Déléguée à la protection des données (*DPO*), sur la base d'un accord de coopération provincial. La *DPO* dispose des compétences requises et exerce la fonction à temps plein mais répartit ses activités sur 14 zones de police. Bien qu'un accord de coopération des DPO puisse effectivement offrir une plus-value et soit salué par le COC, force est de constater que, par le grand nombre de zones de police qui relèvent des attributions de la DPO, celle-ci peut difficilement exercer ses missions de manière effective et efficace. Étant donné son budget-temps limité, la DPO ne peut pas davantage assurer un suivi proactif de la politique en matière de protection des données et de sécurité des informations.

Les aspects de la sécurité des informations, de la protection des données et de l'ICT sont en principe évalués au moins une fois par an (sous la direction du chef de corps). Le coordinateur local/la personne de contact pour la protection des données et la *DPO* prennent part à ces réunions. Pendant la visite, aucun rapport à ce sujet n'a été soumis au COC. Par ailleurs, en application de l'arrêté d'exécution du 6 décembre 2015, la zone de police devait déjà disposer d'un plan de sécurité des informations qui n'avait pas encore été établi au moment de la visite.

Plusieurs mesures ont été mises en œuvre pour garantir l'intégrité, la confidentialité et la continuité des informations et systèmes d'informations. Ces mesures ne font cependant pas l'objet d'une vérification structurelle. Les contrôles internes et *self-assessments* relatifs à la sécurité ICT ne sont pas effectués régulièrement (par exemple, en détectant proactivement des failles dans la protection des logiciels et systèmes informatiques avec des analyses périodiques de la vulnérabilité). Des audits de protection externes n'ont pas été effectués non plus ces dernières années.

Des contrôles proactifs des fichiers de journalisation ne sont pas effectués ; ils interviennent uniquement sur demande. Aucun plan de continuité ICT formel n'a été défini au sein du service ICT. Néanmoins, des actions ont été entreprises à partir du service ICT de la zone de police pour garantir la disponibilité des données numériques et des infrastructures de traitement des informations.

Conclusion – recommandations – mesures correctrices

Conclusion

Seul un nombre minime d'aspects des thèmes contrôlés s'avèrent conformes à la législation. En ce qui concerne les aspects prépondérants sur le plan de la protection des données, il apparaît que la ZP a bien l'ambition de pouvoir apporter une réponse à certaines matières sensibles mais elle en a été empêchée en partie par le budget-temps effectif minime, d'une part, et l'absence d'une documentation détaillée concernant les aspects correspondants, d'autre part (ICT et sécurité des informations), nonobstant l'engagement évident des membres du personnel désignés et de la *DPO*.

La constatation générale précédente traduit les manquements constatés concrets. Surtout dans le domaine de l'utilisation de la surveillance par caméra et de l'application du cadre légal relatif au droit en matière de protection des

[3] Voir la note en bas de page 67.

données, différentes démarches doivent encore être entreprises. En revanche, la ZP affiche un très bon fonctionnement de la gestion fonctionnelle.

Bien que plusieurs directives de corps, relatives à la sécurité des informations, aient été établies, la ZP n'a pas de plan général de sécurité des informations et de continuité, ciblé sur les risques, dans le cadre duquel l'organisation et, en particulier, le service ICT, puisse inscrire ses propres mesures. Une telle approche fondée sur les risques permettrait d'évaluer, de formaliser et de documenter les mesures prises. Le service ICT de la ZP prévoit une série d'initiatives de sécurité ICT mais le contrôle (interne/externe) périodique du bon fonctionnement et de l'exhaustivité de ces initiatives n'est pas assuré d'une manière structurelle et formelle. L'implication de la DPO dans le suivi, la rectification et la mise en œuvre de la politique de sécurité des informations et de protection des données doit être renforcée. Une approche structurelle et un suivi périodique sont indiqués en l'occurrence.

Par conséquent, une série de recommandations s'imposent et doivent contribuer à une amélioration de l'efficacité et de l'efficience du traitement de données (à caractère personnel) par la ZP.

Les manquements légaux constatés incitent cependant l'Organe de Contrôle à prendre des mesures correctrices, la ZP devant régulariser la situation dans un délai déterminé.

Demande

L'Organe de Contrôle demande que le chef de corps, en attendant l'arrêté d'exécution relatif au registre local des caméras, constitue un registre local de l'utilisation de caméras ou l'insère dans un volet séparé du registre des traitements en indiquant clairement les types de caméras, les finalités et le support d'enregistrement des images.

Recommandations

1) Recommandation
En vue d'une application effective et efficace des traitements *ANPR*, il est important que la ZP élabore une politique claire d'intervention pour les *hits* sur les listes nationales et une politique claire d'action et d'intervention sur les listes locales.

2) Recommandation
L'Organe de Contrôle insiste pour l'élaboration d'une *policy/*politique qui permette de mettre en place un mécanisme efficace assurant une surveillance continue des profils et une gestion en temps réel des accès en fonction des effectifs réels.

3) Recommandation
Le COC insiste pour que la ZP définisse dans une note de corps une politique pour la constitution de banques de données particulières reprenant les paramètres sur la base desquels s'opère le contrôle de la conformité de la constitution d'une banque de données particulière pour cette activité de traitement déterminée aux conditions légales de l'article 44/11/3 de la LFP.

4) Recommandation
Il importe que le chef de corps opère, dans l'ordre du corps, une distinction claire entre les divers aspects visés sur le plan de l'accès et de l'utilisation d'Internet et des réseaux sociaux pour des objectifs personnels et professionnels et de l'utilisation ou non d'appareils personnels[4]. C'est ainsi que l'accès à Internet (recherches, sites autorisés et interdits) pendant les heures de service doit être distingué de l'utilisation des réseaux sociaux pendant les heures de service à des fins personnelles, d'une part, et dans la mesure où des informations policières pourraient être partagées, d'autre part. Dans un volet séparé ou un document distinct, l'utilisation d'appareils mobiles privés à des fins opérationnelles et l'utilisation d'appareils mobiles professionnels à des fins personnelles doivent être décrites (séparément). En l'occurrence, il importe que le document décrive clairement ce qui est autorisé et interdit, dans quelles circonstances et à quelles conditions un contrôle peut être effectué, quelles sont les conséquences de la constatation d'infractions au document et les droits de la personne concernée dans ce cadre. Il est donc primordial d'opérer une distinction claire

[4] L'Organe de Contrôle attire l'attention en l'occurrence sur les réglementations légales qui protègent la confidentialité de la communication privée, comme l'article 314bis du Code pénal et la loi du 13 juin 2005 « *relative aux communications électroniques* » qui protège la confidentialité des télécommunications (article 5 de cette loi).

entre les divers aspects et finalités en élaborant une procédure qui définit concrètement les principes de base de la transparence et les droits de la personne concernée. C'est également le cas en ce qui concerne l'utilisation d'images de caméras opérationnelles pour le contrôle du respect des conditions de travail.

5) Recommandation
Le COC insiste sur une rectification du budget-temps pour la *DPO* et sur la limitation du nombre de zones de police pour lesquelles elle exerce un rôle coordinateur en tant que *DPO*, à moins que les *DPO* assistants puissent effectivement exercer leur mission de manière autonome. Le COC estime que, dans les circonstances actuelles, la *DPO* ne peut pas disposer de moyens suffisants (temps) pour exécuter correctement les tâches de *DPO* pour le grand nombre de zones de police dans lesquelles elle a été désignée.

6) Recommandation

Il est recommandé de reprendre les points d'action suivants dans le plan de sécurité des informations :

- la poursuite de l'élaboration et l'affinement de la politique en matière de sécurité des informations et de protection des données par le biais de directives du corps et de procédures. Cette politique doit être réévaluée régulièrement par la direction afin qu'elle reste pertinente, conforme à la réalité. Il est important, en l'occurrence, de communiquer, d'expliquer et de répéter régulièrement les procédures et notes de corps élaborées (au moyen de campagnes de sensibilisation) ;
- les mesures de maturité ainsi que les analyses de risques et de vulnérabilité sont des piliers importants dans la politique de sécurité et contribuent à une sécurité optimale des informations, basée sur les risques. Le budget-temps de la *DPO* fait aussi partie de cette gestion des risques ;
- l'élaboration de procédures formelles de concertation et de communication avec toutes les parties concernées **au sein de la ZP** de telle sorte que la *DPO* soit impliquée davantage dans les activités de l'organisation et dispose toujours des informations nécessaires pour l'exécution de la mission qui lui a été confiée.

7) Recommandation
Il est recommandé d'effectuer une analyse de risque concernant la gestion des fichiers de journalisation et la surveillance des systèmes ICT internes afin d'obtenir les garanties nécessaires relatives à la traçabilité des activités de traitement des données.

8) Recommandation
Le COC insiste pour :

- autoriser exclusivement l'utilisation de comptes d'utilisateur nominatifs/individuels dans le cadre de la gestion opérationnelle. L'utilisation d'un compte d'utilisateur générique pour la gestion système doit être fortement limitée et est autorisée uniquement si elle est requise techniquement ;
- inventorier tous les comptes privilégiés, y compris les comptes de domaine et comptes locaux pour avoir la certitude que seules les personnes autorisées ont des droits majorés ;
- faire en sorte que tous les utilisateurs ayant accès à un compte privilégié utilisent un compte nominatif spécial ou secondaire pour l'exécution d'activités ICT qui nécessitent des droits majorés. Ce compte privilégié peut seulement être utilisé pour ces activités administratives et non pour exécuter des activités opérationnelles quotidiennes, surfer sur Internet, échanger des e-mails ou des activités similaires ;
- reprendre toutes les activités relatives à l'utilisation et à la gestion de ces comptes privilégiés dans des fichiers de journalisation et prévoir des mesures protégeant l'intégrité pour ces fichiers de journalisation.

9) Recommandation
La ZP est encouragée à renforcer la surveillance et les contrôles afin de pouvoir disposer d'une vision correcte et actuelle du fonctionnement et de l'efficacité de la protection intégrale des informations. Cela implique notamment de :

- veiller au respect des obligations légales, réglementaires et contractuelles et de ses propres lignes politiques relatives à la sécurité des informations et, en particulier, au traitement de données à caractère personnel ;

- contrôler régulièrement la conformité des systèmes d'information avec les normes pour l'exécution de la protection et la mesure de la conformité technique. L'exécution de *vulnerability scans*, de *penetration testing* et de *security audit/review* peut notamment être utile à cet effet ;
- une analyse périodique réalisée par un tiers indépendant est une plus-value absolue.

10) Recommandation
Il est recommandé de prévoir un plan de reprise après sinistre ICT (*DRP* ou *Disaster Recovery Plan*) et un plan de continuité pour tous les processus critiques et systèmes essentiels d'information de l'organisation et de les tester sur une base périodique. Un *DRP* pour ICT va bien au-delà de prévoir simplement un *back-up*. Reste à savoir comment préparer l'organisation à tous les sinistres possibles qui peuvent frapper les systèmes ICT.

Mesures correctrices

Étant donné les articles 221 § 1 et 247, 4°, 5° et 6° de la LPD ;

Charge la ZP :

a) de conformer l'accès aux images des caméras avec l'article 25/7 § 1, troisième alinéa de la LFP afin que le motif des consultations soit enregistré. La preuve de cette mise en œuvre conforme à la loi sera soumise dans les neuf mois suivant la date de la notification de cette mesure correctrice à l'Organe de Contrôle ;

b) de tenir à jour les fichiers de journalisation de l'accès aux images des caméras conformément à l'article 56 de la LPD. La preuve de cette mise en œuvre conforme à la loi sera soumise dans les neuf mois suivant la date de la notification de cette mesure correctrice à l'Organe de Contrôle ;

c) d'expliquer les critères d'insertion sur les listes *ANPR* locales et de les transmettre à l'Organe de Contrôle dans les trois mois suivant la date de la notification de cette mesure correctrice à l'Organe de Contrôle ;

d) de consulter régulièrement les journalisations de la BNG et d'effectuer des contrôles proactifs par coups de sonde (2 x/an) dans le but de surveiller l'introduction obligatoire d'un motif de consultation et les consultations irrégulières éventuelles et ce une première fois dans les six mois qui suivent la notification de cette mesure correctrice et d'en mettre leurs résultats à la disposition du COC ;

e) d'établir un plan de sécurité des informations. Le plan de sécurité des informations sera mis à la disposition de l'Organe de Contrôle dans les neuf mois suivant la date de la notification du présent rapport ;

Dit pour droit que la date de début des mesures correctrices et la date de leur notification visée aux lettres a) à e) inclus doit se comprendre comme la date de la transmission du rapport définitif actuel de l'Organe de Contrôle par e-mail contre accusé de réception, augmentée de deux jours.

L'Organe de Contrôle indique la possibilité pour les parties d'interjeter appel dans les trente jours suivant la décision de l'Organe de Contrôle auprès de la cour d'appel du domicile ou du siège du demandeur (article 248 § 1er, premier alinéa et § 2 de la LPD).

RAPPORT

1. INTRODUCTION

1.1. Les compétences de l'Organe de Contrôle

1. La loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après la « LPD »)[5] a réformé l'Organe de contrôle de l'information policière (« Organe de Contrôle » ou « COC »), notamment en une autorité de surveillance à part entière, outre ses compétences de contrôle existantes en matière de traitement policier de l'information tel qu'il est prévu dans la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71, § 1er et les chapitres 2 et 3 du titre VII de la LPD décrivent les missions et compétences du COC. Ils renvoient également aux missions de contrôle spécifiées dans les articles 44/1 à 44/11/13 de la LFP relatifs au traitement de l'information des services de police. De cette manière, l'Organe de Contrôle est investi d'une mission de surveillance et de contrôle. Cela signifie qu'au-delà de la protection de la vie privée et des données à caractère personnel, le COC prête également attention à des éléments tels que l'efficience et l'efficacité du traitement de l'information et de l'intervention policière.

L'Organe de contrôle est compétent pour les services de police[6], pour l'Inspection générale de la police fédérale et de la police locale (AIG)[7] et pour l'Unité d'information des passagers (UIP)[8]. La compétence de surveillance de l'Organe de contrôle à l'égard des services de police couvre à la fois les activités de traitement opérationnelles et non opérationnelles[9]. Enfin, l'Organe de Contrôle est compétent dans le cadre des demandes adressées à l'UIP en matière fiscale à l'égard du Service du Contentieux de l'Administration générale des Douanes et Accises en vertu de l'article 281 § 4 de la loi générale du 18 juillet 1977 *« sur les douanes et accises »*.

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. Au travers d'un examen 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 44/11/13 de la LFP et à leurs mesures d'exécution.

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de Contrôle fonctionne en quelque sorte comme une commission « MAP »[10]. Conformément à l'article 46/6 de la LFP, toute autorisation, et sa prolongation, de l'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 l'autorité 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.

---

[5] *MB*, 5 septembre 2018. Cette loi contient aussi des dispositions d'exécution du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après dénommé « RGPD » et de 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* (*Law Enforcement Directive*).

[6] Tels que définis à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (art. 26, 7°, a de la LPD).

[7] Telle que définie à l'article 2 de 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 (art. 27, 7°, d de la LPD).

[8] Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers (art. 26, 7°, f de la LPD). *BELPIU* est l'acronyme de la dénomination anglaise *Belgian Passenger Information Unit*.

[9] Art. 4 §2, 4ème alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (LAPD).

[10] MAP signifie « méthodes administratives particulières ».

L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé[11]. Les membres de l'Organe de contrôle et les membres du service d'enquête disposent à cet égard de compétences d'investigation et peuvent prendre des mesures correctrices[12].

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 comme en référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire[13].

1.2. Objectifs

2. La surveillance vise à se faire une idée de l'application du cadre légal relatif au traitement de données à caractère personnel, d'une part, et à l'attention de l'entité contrôlée en matière de sécurité des informations, d'autre part. Le respect des procédures et processus de travail joue plutôt un rôle central dans la compétence de contrôle. Néanmoins, les deux compétences ont en commun le traitement de données à caractère personnel.

À la lumière de ce qui précède, l'aspect de la sécurité de l'information dépassera le respect du cadre légal en matière de traitement des données à caractère personnel et/ou de gestion des informations, tel qu'il est stipulé dans la LFP. Il coïncide en effet avec la mise en œuvre et l'application de standards et normes sur le plan de la sécurité de l'information, tant au niveau des processus qu'au niveau des systèmes.

La forme de la surveillance concerne les aspects organisationnels : les différentes étapes dans le processus et le planning correspondant. En l'occurrence, il faut chercher si les activités de traitement répondent au cadre légal du RGPD, de la LPD et de la LFP et aux exigences en matière de sécurité de l'information en ce qui concerne la structure, les processus de traitement et les systèmes.

2. CONCEPTION DE LA VISITE ET MÉTHODOLOGIE

2.1. Contexte

3. Le 28 octobre 2020, l'Organe de Contrôle a rendu une visite à une ZP dans la province du Limbourg. La visite s'est déroulée dans le cadre du Plan stratégique de l'Organe de Contrôle qui prévoit de visiter chaque année plusieurs zones de police et/ou entités de la police fédérale en vue de l'exécution des compétences de contrôle et de surveillance exposées précédemment. La visite n'était donc pas la conséquence d'une plainte (individuelle) ou de l'existence d'indices (concrets) à propos du non-respect de la législation et de la réglementation par le service de police local visité.

Avec l'introduction du RGPD et de la LPD, il règne beaucoup d'inquiétude au sein des services de police quant à l'application correcte du cadre légal et des questions à ce propos. Cela ressort de la multitude de questions à l'Organe de Contrôle, sur le plan des activités de traitement, tant opérationnelles que non opérationnelles, comme le traitement de données à caractère personnel et le contrôle des prestations de travail du personnel. Par ailleurs, de nombreuses zones de police sont confrontées à la complexité du cadre légal modifié en 2018 pour l'installation et l'utilisation de caméras. Par conséquent, l'approche de la visite met l'accent sur la *sensibilisation,* en ce qui concerne l'application du RGPD, de la LPD et de la législation sur les caméras, et est *compliance-based*, en ce qui concerne le contrôle de la qualité des enregistrements dans la BNG. Ces deux facettes de l'approche n'empêchent cependant pas que l'Organe de Contrôle prenne et doive prendre des mesures adéquates lorsque des infractions et/ou manquements légaux évidents sont constatés.

[11] Art. 240, 4° de la LPD.

[12] Art. 244 et 247 de la LPD.

[13] Art. 248 de la LPD.

4. Étant donné cette réalité complexe, le choix s'est porté sur l'exécution d'une visite en largeur (visite globale). Cela signifie que la visite a porté sur plusieurs thèmes sans trop approfondir les thèmes individuels. En l'occurrence, une attention particulière a été accordée à l'application du cadre juridique en matière de protection des données, en général, et de sécurité des informations, en particulier. En tant que notion faîtière, la sécurité des informations a en effet un impact sur l'intégrité, la fiabilité, la confidentialité et la disponibilité des données pour la police. En l'occurrence, un rôle important est dévolu au délégué à la protection des données (*DPO*, *Data Protection Officer*). Cette fonction se voit attribuer un rôle de conseil et de contrôle à l'égard du responsable (opérationnel) du traitement et fonctionne sur ce plan comme l'interlocuteur de l'Organe de Contrôle.

La visite comprenait cinq thèmes :

1) l'utilisation de caméras ;
2) le contrôle de la gestion des données et des informations dans la BNG ;
3) les banques de données particulières ;
4) les systèmes de contrôle du personnel ;
5) la sécurité des informations : organisation, politique et gestion ICT.

2.2. Méthodologie

5. La visite se composait de deux phases. Dans la première phase, un questionnaire a été remis à la zone de police pour obtenir les informations et documents nécessaires à propos des cinq thèmes indiqués. En fonction du contenu des réponses ou de leur absence (partielle), une *shortlist* (une sélection parmi les réponses au questionnaire) a été établie. De cette manière, la visite des lieux a pu être réduite à un laps de temps minimal.

6. La deuxième phase portait sur la visite sur place (la « visite » proprement dite). Celle-ci a été scindée en sept parties.

1) Visite dans la zone de police :
   - un aperçu des différents services ;
   - une visite au dispatching en ce qui concerne le traitement des images des caméras ;
   - l'infrastructure ICT dans le cadre de la sécurité des informations.
2) L'utilisation de la surveillance par caméra :
   - caméras *ANPR* le long des voies d'accès de la ville ;
   - la surveillance par caméra dans la ville ;
   - la surveillance par caméra dans le complexe de cellules.
3) Le traitement des données dans la BNG, en particulier :
   - journalisation ;
   - profils ;
   - validation centrale ;
   - contrôle de qualité.
4) Banques de données particulières.
5) L'utilisation d'appareils mobiles dans le cadre ou non de missions opérationnelles, en particulier :
   - utilisation d'*ordinateurs portables* ou de *smartphones* pour des missions opérationnelles ;
   - utilisation d'*ordinateurs portables* ou de *smartphones* à des fins non-opérationnelles.
6) Le traitement de données biométriques à des fins non-opérationnelles.
7) Contrôle du registre des traitements et du registre en matière de surveillance par caméra.

À cette occasion, la sécurité des informations, tout comme le rôle actif du *DPO*, ont été analysés à partir d'une approche générique.

Un aspect de la visite réside dans la tendance à l'utilisation d'appareils mobiles (*smartphones*, *i-pad*, *ordinateurs portables*…) à des fins opérationnelles (point 5). Cet aspect peut être réparti entre l'utilisation d'appareils privés et l'utilisation d'appareils mobiles mis à disposition par la police. Par « fins opérationnelles », il faut entendre l'utilisation d'appareils mobiles pour des activités de police opérationnelles, comme la prise de photos ou de copies de documents et les traitements administratifs opérationnels effectués dans leur prolongement, comme l'envoi de messages e-mail avec des informations policières.

Ensuite, la zone de police a eu la possibilité de formuler des remarques sur le rapport et/ou d'indiquer sur quels points ont entre-temps été prises toutes les actions de remédiation qui exercent une influence sur les recommandations et/ou mesures correctrices envisagées. La ZP a fait usage de cette possibilité dans le délai imposé. Lorsqu'elles étaient pertinentes, ces remarques ont été prises en compte.

3. DISPOSITIONS LÉGALES ET RÉGLEMENTAIRES PERTINENTES

3.1. Généralités

7. Pour les thèmes opérationnels qui ont fait l'objet de la visite et en constituent la majeure partie, deux réglementations légales sont prépondérantes : la loi du 30 juillet 2018 relative à la protection des données à caractère personnel (LPD) évoquée précédemment et la loi sur la fonction de police (LFP). La loi d'adaptation du 21 mars 2018[14] de la LFP est d'application depuis le 25 mai 2018 à l'utilisation de la surveillance par caméra par les services de police. Elle prévoit toutefois une disposition transitoire de 12 mois pour donner aux services de police le temps de se mettre en règle avec ces modifications de loi.

8. En ce qui concerne l'utilisation d'appareils (privés) à des fins non-opérationnelles, le cadre légal général du RGPD et de la LPD est d'application. C'est aussi le cas lorsque, par exemple, des données biométriques[15] sont traitées à des fins non-opérationnelles ou des images de caméras (policières) sont utilisées pour le contrôle du respect des conditions de travail du personnel de la police[16]. Étant donné la complexité des traitements policiers et non policiers, une brève explication est donnée ci-après au point 3.2.

3.2. Activités de traitement policières et non-policières

9. Sur le plan du traitement des données à caractère personnel, les tâches et missions d'un service de police comprennent globalement deux domaines : les traitements policiers (à savoir, la police administrative et judiciaire) et ordinaires (administratifs) ou non-policiers. Des exemples de ces derniers sont la gestion du personnel et d'autres activités de traitement administratives et logistiques par la police. Sur le plan de la transparence et des droits de la personne concernée, les traitements policiers sont soumis à des restrictions (d'envergure) alors que ce n'est en principe pas le cas pour les traitements non policiers. Cela revient à soumettre le contrôle du fonctionnaire de police dans le cadre de la relation de travail (traitement non-policier) aux dispositions du RGPD et aux dispositions d'exécution telles qu'elles sont stipulées dans le titre 1 de la LPD. Des exemples sont le contrôle de l'utilisation d'Internet et de la messagerie électronique (à des fins personnelles), le traitement de catégories particulières de données à caractère personnel, telles que les empreintes digitales, dans le cadre de la politique du personnel et de l'utilisation de la surveillance par caméra dans le contexte du droit du travail. En ce qui concerne le traitement de données biométriques dans le cadre de la politique du personnel, l'Organe de Contrôle a déjà considéré dans différents dossiers que, dans l'état actuel de la législation, il manque un fondement légal suffisant et adéquat (voir plus loin la rubrique 4.5.1). Le titre 2 de la LPD et la LFP sont d'application aux traitements policiers, comme indiqué précédemment[17].

10. Cette législation complexe repose sur l'assistance du délégué à la protection des données (*DPO*). D'importantes missions sont confiées au *DPO* par la LPD. Le *DPO* ne fournit pas seulement une assistance sur demande au responsable du traitement (opérationnel). Il doit également veiller au respect de la législation applicable et des règles internes[18]. Il ne peut par conséquent pas adopter une attitude attentiste. Cela signifie que le *DPO* contrôle proactivement, via une

[14] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.* 16 avril 2018.
[15] Art. 4.14 RGPD :
« *«données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques*. Il s'agit en d'autres termes de l'identification unique ou l'authentification de la personne (considération 51, RGPD).
[16] Voir l'Avis d'initiative concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail (BD20007), à consulter sur https://www.organedeContrôle.be/files/BD200007_Surveillance_Camera_Lieu_de_Travail_Avis_dOffice_17-08-2020_00016316.PDF.
[17] Voir notamment pour plus d'explications à propos de la distinction entre les traitements policiers et non policiers, R. SAELENS, 'Europa zet de bakens uit voor de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie: een beknopte verkenning van de Richtlijn politionele en Justitiële verwerkingen', *P&R* 2019, livr. 2, 51-70.
[18] Art. 65 de la LPD.

surveillance interne, si les conditions pour un traitement sûr et légitime des données à caractère personnel sont respectées (voir plus loin).

3.3. Surveillance par caméra et application de la LPD

11. Depuis la loi d'adaptation du 21 mars 2018, la décision de placer des caméras dans les espaces publics ne peut plus être prise que par une autorité publique, comme la commune[19]. Lorsque la police utilise la surveillance par caméra, les dispositions de la LFP sont d'application, sauf si l'utilisation de caméras est régie par une autre législation[20].

3.3.1. Responsable du traitement

12. Dans le droit relatif à la protection des données, un rôle important est dévolu au « responsable du traitement ». Il s'agit de « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »[21]. En ce qui concerne les activités de traitement dans le cadre des missions de police administrative et judiciaire, le responsable du traitement est défini dans la LPD comme « *l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l'ordonnance, le responsable du traitement est l'entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance* »[22]. Par « *autorité compétente* », il faut entendre « *a) 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* »[23].

6. Bien que le responsable du traitement dans la LFP se voie attribuer un rôle (spécifique) à certains endroits, ce n'est pas le cas en ce qui concerne l'utilisation de caméras. Comme indiqué précédemment, le responsable du traitement est un acteur essentiel dans le traitement des données à caractère personnel. Il doit en effet démontrer que les données à caractère personnel sont traitées conformément au cadre légal. Lui, son préposé ou mandataire, est aussi la personne à laquelle des mesures correctrices éventuelles peuvent être imposées ou qui peut être poursuivi pénalement[24].

Le chef de corps est le responsable du traitement pour l'enregistrement d'images de caméras dans une banque de données technique locale[25]. Le chef de corps est aussi le responsable du traitement pour les banques de données particulières[26].

3.3.2. Exigences procédurales

[19] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, M.B. 16 avril 2018.
[20] Comme le contrôle de tronçon, qui relève de l'application de la loi du 16 mars 1968 relative à la police de la circulation routière (Doc. parl. Chambre 2017-2018, n° 54-2855/001, 9).
[21] Art. 4. 7) du RGPD.
[22] Art. 26, 8° de la LPD.
[23] Art. 26, 7° de la LPD.

[24] Voir les articles 221 et 222 de la LPD. Concrètement, l'Organe de contrôle peut notamment prendre les mesures suivantes (art. 25.2, RGPD) : - donner un avertissement ; - donner une réprimande ; - ordonner de mettre les opérations de traitement en conformité avec le cadre légal dans un délai déterminé ; - imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement.

[25] Art. 44/11/3*sexies* § 1, 2e alinéa de la LFP.
[26] Article 44/4 § 1, troisième alinéa de la LFP.

14. Avant qu'un service de police puisse installer des caméras de surveillance sur le territoire d'une commune, il a besoin à cet effet de l'autorisation de principe du conseil communal[27]. Toutefois, une autorisation n'est pas nécessaire pour l'utilisation de caméras dans des lieux fermés dont la police elle-même est le gestionnaire, comme un commissariat de police[28]. Il importe de préciser que, lorsque l'autorisation du conseil communal a déjà été obtenue avant la modification de loi du 21 mars 2018 en application de la loi sur les caméras de 2007, il ne faut pas obtenir une nouvelle autorisation du conseil communal[29]. Cette autorisation initialement obtenue reste donc valable. La même autorisation ne peut toutefois pas être employée pour l'utilisation de nouveaux types de caméras qui ont été introduits par la loi du 21 mars 2018. C'est ainsi que la LFP impose des conditions spécifiques à l'utilisation de caméras fixes temporaires sur lesquelles le conseil communal doit se prononcer[30]. Dans ce cas, il faut donc obtenir une autorisation nouvelle, ou complémentaire, du conseil communal.

3.3.3. Délai de conservation des images

15. Les images des caméras peuvent être conservées pour une durée n'excédant pas douze mois[31]. La loi ne fixe pas de délai minimum. En ce qui concerne les images de caméra classiques, la LFP ne spécifie pas sur quel support de données les images doivent être enregistrées. Par conséquent, il est indiqué que le chef de corps indique dans le registre relatif au traitement de données à caractère personnel, tel qu'il est visé dans l'article 55 de la LPD (voir numéro 3.3.8), sur quel support de données les images sont enregistrées. Ce support de données doit être accessible pour l'Organe de contrôle.

3.3.4. Banques de données techniques

16. Un régime spécifique est d'application pour l'utilisation de caméras ANPR. Il s'agit de « caméras intelligentes », à savoir des « *caméras qui comprennent également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies* »[32]. Lorsque des caméras de surveillance ANPR sont utilisées, les images doivent être traitées dans une *« banque de données technique »*,[33] les données à caractère personnel et les informations étant également transmises à la banque de données technique nationale[34]. Les images peuvent être conservées pour une durée n'excédant pas douze mois sans qu'un délai minimum ne soit spécifié ici non plus[35].

La banque de données technique contient les données suivantes, si elles apparaissent sur les images[36] :

1) la date, le moment et l'endroit précis du passage de la plaque d'immatriculation,
2) les caractéristiques du véhicule lié à cette plaque,
3) une photo de la plaque d'immatriculation à l'avant du véhicule et le cas échéant, à l'arrière,
4) une photo du véhicule,
5) le cas échéant, une photo du conducteur et des passagers,
6) les données de journalisation des traitements.

Ces données doivent donc être traitées dans la banque de données technique pour autant qu'elles apparaissent sur les images *ANPR*.

3.3.4. Accès aux images

[27] Art. 25/4 § 1, 1° de la LFP.
[28] Exposé des Motifs de cette loi, p. 21 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).
[29] Art. 88 de la loi du 21 mars 2018 et Exposé des Motifs de cette loi, p. 113-114 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).
[30] Art. 25/4 § 2, 2e alinéa de la LFP.
[31] Art. 25/6, 44/11/3*decies* § 2, alinéa premier, et 46/12, alinéa premier de la LFP.
[32] Art. 25/2 § 1, 3°, *juncto* 44/2 § 3, troisième alinéa de la LFP.
[33] Art. 44/2 § 3, alinéa premier de la LFP.
[34] Art. 44/11/3*sexies* de la LFP.
[35] Art. 44/11/3*decies* § 2, alinéa premier de la LFP.
[36] Art. 44/11/3*decies* § 1 de la LFP.

17. L'accès aux images dépend de la finalité et est réglé de la même manière tant pour la surveillance par caméras ordinaires que pour l'utilisation de caméras *ANPR*. Dans les deux cas, les images peuvent être conservées pendant 12 mois maximum. En ce qui concerne les missions de police administrative, l'accès est limité au premier mois suivant l'enregistrement des images. Pour les missions de police judiciaire, les images sont accessibles pendant toute la durée de leur conservation mais l'intervention du procureur du Roi est nécessaire après le premier mois[37]. L'accès doit être motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise[38]. Autrement dit, l'accès aux images est autorisé uniquement aux personnes qui ont besoin de ces données à caractère personnel et informations et lorsqu'un intérêt opérationnel concret est donc présent à cet effet[39].

3.3.6. Utilisation visible et non visible de caméras

18. Les caméras visibles sont les caméras dont l'utilisation est signalée par des pictogrammes, les caméras montées à bord de véhicules de police, de navires de police, d'aéronefs de police, ou de tout autre moyen de transport de police ou portées par des fonctionnaires de police qui sont identifiables comme tels[40]. Dans des situations exceptionnelles, la police peut faire un usage dissimulé de caméras (utilisation non visible). Dans ce cas, la caméra est portée par le fonctionnaire de police ou placée dans un véhicule de police banalisé. Il est question d'un véhicule de police banalisé lorsque le véhicule de police n'est pas reconnaissable en tant que tel. Dans ce cas, il est donc question d'utilisation « *non visible* » de la caméra[41]. L'application de caméras non visibles est régie strictement et se limite à quatre situations. À savoir :
1) en raison de circonstances particulières, notamment en cas d'attroupements, en vue de recueillir des informations de police administrative sur des personnes radicalisées ou *terrorist fighters,* et de véhicules de police banalisés pour la lecture automatique de plaques d'immatriculation, en vue de détecter des véhicules signalés. (art. 46/4 LFP) ;
2) pour la préparation d'actions de police judiciaire ou pour le respect de l'ordre public pendant ces actions (articles 46/7 et 46/8 LFP) ;
3) dans le cadre de missions spécialisées de protection des personnes (art. 44/9 LFP) et
4) pendant le transfert de personnes détenues ou arrêtées (art. 46/11 LFP).

Sauf si l'utilisation non-visible de caméras est effectuée sous l'autorité d'un magistrat, cette forme d'utilisation de caméras doit toutefois être notifiée préalablement à l'Organe de contrôle. Cette notification préalable doit permettre à l'Organe de contrôle d'apprécier la légalité de la décision[42].

3.3.7. Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou *DPIA, Data Protection Impact Assessment*)

14. Depuis la loi du 21 mars 2018, il est obligatoire d'établir une analyse d'impact et de risques préalablement à l'utilisation de caméras de surveillance, la protection de la vie privée étant mise en balance avec le niveau opérationnel de l'utilisation des caméras[43]. Cet exercice doit également être établi avant la constitution d'une banque de données technique (locale)[44]. À cet effet, l'assistance du *DPO* est demandée[45].

Sous réserve que les conditions de la LPD pour une *DPIA* et les conditions pour une analyse d'impact et de risques concernant l'utilisation visible de caméras et/ou concernant la constitution des banques de données techniques en vertu de la LFP soient satisfaites, les deux analyses peuvent être réunies en un seul document. Étant donné qu'une DPIA en vertu de la LPD nécessite une analyse plus large que celle prescrite dans la LFP, il est indiqué que, dans le cas où les deux sont traitées ensemble, cette analyse doit, conformément à la LPD, couvrir tous les systèmes et procédures pertinents d'activités de traitement. Hormis le respect de la LPD et de la LFP, les mesures de précaution opérationnelles et les mesures de protection (qui sont prises pour limiter les risques pour les données à caractère personnel à protéger) doivent également être décrites.

---

[37] Art. 25/7 § 1, 1er et 2e alinéas et 44/11/3*decies* § 3, deuxième alinéa de la LFP.
[38] Art. 44/11/3*decies* § 3, 1er alinéa de la LFP.
[39] Exposé des Motifs de cette loi, p. 29 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).
[40] Art. 25/2 § 2 de la LFP.
[41] Art. 46/4 et suiv. de la LFP.
[42] Art. 46/6 et 46/10 de la LFP.
[43] Art. 25/4 § 2 de la LFP.
[44] Art. 44/11/3*octies* de la LFP.
[45] Art. 65, 3° *juncto* 58 de la LPD.

3.3.8. Registre

20. L'utilisation de la surveillance par caméra doit être consignée dans un registre (local)[46]. Le registre indique le type de caméras et leur localisation. Cependant, aucun arrêté royal n'a encore été promulgué pour préciser le contenu de ce registre. Néanmoins, l'Organe de Contrôle estime qu'à la lumière de l'efficacité de ses compétences de surveillance, le service de police, en l'attente de l'arrêté d'exécution, doit constituer de sa propre initiative un registre qui reprend toutes les utilisations de (types de) caméras, y compris l'utilisation non-visible de caméras. De cette manière, l'Organe de Contrôle (et, du reste, la zone de police elle-même, en premier ressort) se fait une vue d'ensemble et une idée de l'utilisation de la surveillance par caméra sur le territoire de la commune qui relève de la compétence du service de police. Dans le même temps, l'utilisation de caméras de surveillance peut être contrôlée en fonction du registre des activités de traitement (voir plus loin). Étant donné que des données à caractère personnel sont traitées par la caméra, ce traitement doit également figurer dans le registre des activités de traitement[47]. Les deux registres sont ou doivent être disponibles pour l'Organe de contrôle.

3.3.9. Journalisation

21. La police est tenue de tenir des fichiers de journalisation[48]. Un fichier de journalisation est un instrument par excellence pour contrôler la preuve de la licéité (ou l'illicéité) du traitement et garantir l'intégrité et la protection des données[49]. Sur ce plan, les fichiers de journalisation sont importants également en cas de procédures disciplinaires internes ou d'enquêtes administratives. Les fichiers de journalisation sont par conséquent essentiels en vue du contrôle tant proactif que réactif et ce, tant au niveau interne qu'externe.

22. Les fichiers de journalisation doivent être distingués de l'identifiant ou de l'accès au système de traitement pour pouvoir consulter les données. En ce qui concerne l'accès aux images caméra (des caméras de ville et du bâtiment de la police), la LFP ne contient pas de réglementation spécifique relative aux profils qui ont accès aux images caméra. En règle générale, l'accès aux images est sécurisé et la raison concrète de l'accès est enregistrée[50]. Néanmoins, les règles générales de la LPD et les dispositions spécifiques de la LFP sont d'application sur ce plan. Cela signifie que l'accès aux images n'est autorisé qu'aux personnes qui ont besoin de données à caractère personnel et d'informations lorsqu'un intérêt opérationnel concret est présent à cet effet et que l'accès est traçable[51].

3.4. Gestion fonctionnelle

23. Les données policières et judiciaires sont particulièrement sensibles. Elles ne peuvent être traitées que dans le cadre de missions de police judiciaire ou administrative, conformément aux prescriptions légales (LFP, LPD, MFO 3[52], le Code d'Instruction criminelle, le secret professionnel, le secret de l'instruction, etc.). Par conséquent, toute utilisation des applications liées à la BNG (enregistrement ou modification d'une donnée, consultation, etc.) couplée à des profils d'accès et à l'accès aux données est tenue dans un fichier de journalisation. Il en va de même pour toute utilisation du Registre national ou des données de la DIV[53]. Les traitements exécutés dans les banques de données de base font également l'objet de fichiers de journalisation qui sont conservés pendant quinze ans à partir du traitement exécuté dans les banques de données de base. Le responsable du traitement peut, si nécessaire, prolonger ce délai d'une période maximale de quinze ans[54].

---

[46] Art. 25/8 de la LFP.
[47] Art. 55 de la LPD.
[48] Art. 56 § 1 de la LPD, en exécution de l'article 25 de la Directive Police & Justice et de l'art. 44/11/3decies § 1, 6° de la LFP.
[49] Art. 56 § 2 de la LPD.
[50] Art. 25/7 § 1, 3e alinéa, 44/4 § 2, 2e et 3e alinéas 44/11/3*novies* de la LFP. Ces derniers imposent la tenue de journaux pour le traitement de données à caractère personnel et des informations dans les banques de données (techniques) opérationnelles.
[51] Voir supra et l'Exposé des Motifs de la loi du 21 mars 2018, p. 29 et 30 (Doc. Parl. *Chambre* 2017-2018, n° 54-2588/001).
[52] La directive commune MFO 3 des ministres de la Justice et de l'Intérieur « relative à la gestion des informations en matière de police judiciaire et administrative ».
[53] Direction pour l'Immatriculation des Véhicules.
[54] Art 44/11/2 §8 LFP.

La directive ministérielle MFO 6[55] régit les huit fonctionnalités de base[56] du fonctionnement des CIA. Dans le cadre de l'organisation et de la substitution des flux d'information, le CIA doit jouer un rôle important de soutien en faveur des gestionnaires fonctionnels dans les zones de police. Ce soutien s'exprime au niveau de l'accompagnement, du contrôle de qualité et du suivi des problèmes remarqués ou signalés.

4. CONCLUSIONS DES RECHERCHES ET ANALYSE JURIDIQUE

4.1. Traitements policiers

4.1.1. L'utilisation de la surveillance par caméra classique et des caméras ANPR : approbation du conseil communal

24. La ZP dispose de plusieurs caméras fixes en vue du contrôle d'un nombre limité de lieux publics (espace public), dans le commissariat de police, 3 caméras *ANPR* fixes à la frontière Belgique - Pays-Bas et inversement ainsi que 1 caméra *ANPR* mobile. Il ressort des constatations que les caméras *ANPR* fixes ont été approuvées par 2 décisions du Conseil communal :

- Conseil communal du 19 décembre 2017 ;
- Conseil communal du 22 mai 2018 ;

25. L'approbation du Conseil communal à l'audience du 19 décembre 2017 concerne 1 caméra *ANPR* à hauteur de la frontière[57]. L'approbation du conseil communal à l'audience du 22 mai 2018 concerne la reprise des 2 caméras *ANPR* de la police fédérale à l'autre frontière.

26. En revanche, aucune approbation du Conseil communal n'a été produite à l'Organe de Contrôle pour l'installation et l'utilisation de caméras fixes qui sont utilisées exclusivement par la police pour exercer un contrôle sur les lieux publics. Par ailleurs, la ZP a 1 caméra *ANPR* mobile visible, montée dans un véhicule de police identifiable comme tel. Celle-ci est utilisée pour l'enregistrement automatique de plaques d'immatriculation de véhicules signalés. Pour cette caméra *ANPR* mobile, la ZP ne disposait pas non plus d'une approbation du conseil communal. **De ce fait, l'utilisation de caméras fixes en vue de la surveillance de l'espace public et l'utilisation de la caméra *ANPR* mobile n'étaient pas conformes à l'article 25/4 § 1, 1° de la LFP.**

En réponse au projet de rapport, il est signalé que la ZP a reçu le 24 novembre 2020 le consentement du conseil communal pour l'utilisation de ces caméras. L'Organe de Contrôle prend connaissance de l'arrêté du conseil communal et, à ce propos, biffe la mesure correctrice envisagée du projet de rapport (désignée dans le projet comme la mesure « a ») concernant les caméras fixes en vue de l'exercice d'une surveillance de l'espace public et la caméra *ANPR* mobile.

4.1.2. Responsable du traitement pour les caméras *ANPR* fixes

27. La visite sur place a permis de constater que la police supposait que les deux caméras *ANPR* fixes à la frontière avec les Pays-Bas ne relevaient pas de la responsabilité de la ZP. La ZP renvoie à ce sujet à la décision d'approbation du 22 mai 2018 mentionnée au numéro 24.

28. Il ressort de l'arrêté que la zone de police reprend deux caméras *ANPR* fixes de la police fédérale. Les images des caméras ANPR ne sont pas conservées sur le serveur de la ZP mais bien au backoffice central de la police fédérale du

[55] Directive commune et contraignante MFO 6 des ministres de la Justice et de l'Intérieur relative au fonctionnement et à l'organisation des carrefours d'informations de l'arrondissement (CIA).
[56] Ces huit fonctionnalités de base sont :
1. Suivi des événements et faits qui se sont produits récemment afin de détecter et d'identifier rapidement les problèmes de sécurité supralocaux
2. Identification des relations entre événements ou faits et antécédents
3. Appui à la coordination et au suivi des enquêtes annoncées
4. Suivi des événements et faits dans le temps et dans l'espace
5. Appui dans le cadre du suivi intégré de phénomènes
6. Appui au suivi des groupes d'auteurs et de victimes
7. Contribution à l'échange transfrontalier de données policières
8. Appui aux gestionnaires fonctionnels du traitement de l'information au sein des zones de police
[57] Remarquez que, d'un point de vue strictement juridique, l'« acceptation » de l'achat de caméras, en soi, n'implique pas du même coup l'« approbation » de l'installation et de l'utilisation des caméras, telle que visée à l'article 25/4 § 1, 1° de la LFP.

Limbourg (CSD/SICAD)[58]. Étant donné que la ZP ne conserve pas les images et n'a pas d'accès direct aux images conservées, la ZP suppose qu'elle ne peut être considérée comme le responsable du traitement.

29. L'Organe de Contrôle ne peut adhérer à la vision de la ZP. Il ressort de la décision du conseil communal que les 2 caméras *ANPR* fixes ont été cédées à la ZP si bien qu'elle doit en être considérée pour le moment comme le responsable du traitement. À compter de cet instant, la police fédérale n'a en effet plus de contrôle sur ces deux caméras *ANPR* fixes (la police fédérale ne détermine en effet pas (plus) la finalité et les moyens). La décision d'utiliser ou non les caméras *ANPR* appartient en effet complètement à la ZP. Le fait que la ZP elle-même n'ait pas accès aux images des caméras n'est pas une condition nécessaire pour qu'elle soit considérée comme le responsable du traitement. Dans le cadre de la LFP, il n'est en effet pas requis que la police locale conserve elle-même les images. La ZP *peut* constituer une banque de données technique locale (dans laquelle les images et les données correspondantes sont conservées) mais ne doit pas forcément le faire. En tout cas, les images doivent être transmises directement à la banque de données technique nationale[59]. Pour la conservation des images (et des données correspondantes) dans la banque de données technique nationale, les ministres de l'Intérieur et de la Justice sont en revanche bien désignés comme les responsables du traitement[60], même s'il s'agit de caméras *ANPR* qui sont placées et utilisées par la police locale.

30. Que les images aient (encore) été conservées provisoirement au backoffice de l'arrondissement ne change rien à la constatation que la ZP doit être considérée comme le responsable du traitement pour les caméras *ANPR* à la frontière avec les Pays-Bas. Par conséquent, c'est bien le cas pour la caméra *ANPR* à la frontière, qui a été approuvée par l'arrêté du conseil communal du 19 décembre 2017 mentionné au numéro 24, bien qu'en vertu de l'arrêté, les « *HITS op de genoemde blacklist (…) via de Centrale Back Office worden doorgestuurd naar het bevoegde CIC (…)*» (traduction libre : les HITS sur ladite *blacklist* (…) sont transmis par le Back Office central au CIC compétent).

4.1.3. Délai de conservation des images et banque de données technique

31. Les images ordinaires des caméras fixes (cellules de police, bâtiment de la police et espace public) sont conservées sur un serveur local de la police pendant 26 jours maximum en moyenne. Ce court délai de conservation est imputable à une capacité de stockage limitée imposant d'écraser ces images par de nouvelles après ce délai[61].

32. Les images de la caméra *ANPR* mobile ne sont pas conservées sur un serveur distinct. Des hits sont générés mais ceux-ci ne sont pas transmis à une autre banque de données technique (nationale). Étant donné que la corrélation est opérée sur une application sur l'ordinateur portable dans le véhicule et que cette application traite les listes nécessaires pour pouvoir effectuer la corrélation, il faut cependant considérer l'ordinateur portable comme une banque de données technique locale pour les images *ANPR* mobiles. **La ZP dispose donc d'une banque de données technique locale pour les images *ANPR* mobiles (voir plus loin 4.1.7).**

4.1.4. Cellules de police

33. L'Organe de Contrôle a pu constater que la surveillance par caméra était appliquée dans les cellules de police dans le bâtiment de la police de la ZP conformément à l'article 10 de l'arrêté royal du 14 septembre 2007[62].

4.1.5. Autres types de surveillance par caméra

34. Selon la ZP, d'autres formes de surveillance par caméra, telles que l'utilisation de *bodycams* ou l'utilisation invisible de caméras, ne sont pas appliquées. Confrontée à l'information d'un communiqué de presse de 2016 annonçant l'utilisation (invisible) de caméras fixes mobiles et déplaçables par la ZP en vue de lutter contre les nuisances et décharges sauvages, la ZP a communiqué au COC que cela n'avait eu lieu qu'une seule fois. Cette pratique a été interrompue parce qu'il s'est avéré que l'utilisation de caméras n'était pas conforme à la législation en vigueur. L'Organe de Contrôle en prend acte.

[58] Voir la rubrique 3.3.1.
[59] Art. 44/11/3sexies § 2 de la LFP
[60] Art. 44/11/3sexies § 1 de la LFP.
[61] Par l'« écrasement » des images, l'emplacement de ces images est occupé par de nouvelles.
[62] A.R. du 14 septembre 2007 relatif aux normes minimales, à l'implantation et à l'usage des lieux de détention utilisés par les services de police, *M.B.* 16 octobre 2007.

4.1.6. Accès aux images (identifiant) et connexion (moment, motif de la consultation)

35. Dans la ZP, l'accès aux images des caméras ne dépend pas du type d'utilisation des caméras. Les images des caméras dans la ville, du complexe de cellules et la surveillance du bâtiment de la police sont accessibles au personnel opérationnel sur la base d'un identifiant général de service et d'un mot de passe.

L'utilisation d'un identifiant général de service n'est pas conforme aux obligations légales. Cela signifie qu'un accès individualisable aux images des caméras n'est pas utilisé. Par ailleurs, aucun fichier de journalisation de l'accès aux images n'est tenu. L'Organe de Contrôle a par conséquent constaté que l'accès aux images des caméras ne pouvait être contrôlé, ce qui ne permet pas de contrôle de la licéité (ou l'illicéité) de l'accès aux images des caméras, alors qu'il s'agit pourtant d'une obligation légale[63].

36. La ZP ne disposait pas d'une gestion adéquate des accès et des utilisateurs aux images des caméras. Cette situation est problématique, comme l'a illustré clairement le manquement constaté sur ce plan en matière d'accès aux images des caméras.

Mesure correctrice
L'accès aux images des caméras doit être conformé à l'article 25/7, § 1er, 3e alinéa de la LFP de telle sorte que le motif des consultations soit enregistré. La preuve de cette mise en œuvre conforme à la loi sera soumise à l'Organe de Contrôle dans les neuf mois qui suivent la date de la notification de cette mesure correctrice à l'Organe de Contrôle.

Mesure correctrice
Les fichiers de journalisation doivent être tenus conformément à l'article 56 de la LPD. La preuve de cette mise en œuvre conforme à la loi sera soumise à l'Organe de Contrôle dans les neuf mois qui suivent la notification de cette mesure correctrice.

4.1.7. Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou *DPIA, Data Protection Impact Assessment*)

37. La ZP a soumis une *DPIA* pour (les différentes formes de) l'utilisation de caméras dans la zone de police. Le COC fait toutefois remarquer qu'en ce qui concerne les caméras *ANPR* locales, on ne peut s'appuyer sur la *DPIA* de la banque de données technique nationale (AMS[64]). La *DPIA* de l'AMS ne porte pas sur les caméras (des zones de police locales) en tant que telles. Le COC a constaté que, **préalablement à la constitution de la banque de données technique locale (voir 4.1.3), aucune DPIA n'avait été établie alors qu'il s'agit d'une obligation légale[65].** La *DPIA* date en effet du 27 octobre 2020 alors que la ZP utilisait déjà une caméra *ANPR* mobile depuis longtemps avant la visite.

Les *DPIA* établies par la ZP pour l'utilisation des caméras sont soumises à une analyse *prima facie*[66]. L'Organe de Contrôle a trois remarques générales. D'une part, le personnel de la police intégrée ne peut être considéré comme un « sous-traitant ». Il s'agit en l'espèce de préposés qui disposent de droits d'accès pour pouvoir effectuer leur mission. Il n'en va pas de même des prestataires de services externes (fournisseurs) qui ont accès aux données dans le cadre de leurs accords contractuels. Ensuite, le citoyen n'a pas de droit d'« objection » aux traitements régis par la loi (LFP)[67]. Enfin, les dispositions transitoires de l'article 284 LPD[68] ne peuvent être invoquées pour les banques de

[63] Art. 25/7 § 1, 3e alinéa LFP et 56 LPD. Par souci d'exhaustivité, il faut remarquer que la police ne peut se prévaloir de l'article 284 de la LPD. En vertu de cette disposition, les systèmes de traitement automatisés qui ont été mis sur pied avant le 6 mai 2018 par la ZP – en l'espèce – ne seront conformés à l'article 56, § 1 de la LPD (fichiers de journalisation) que pour le 6 mai 2023 au plus tard. Étant donné que le réseau de caméras n'a été installé par la zone de police qu'après le 6 mai 2018 et, en tout cas, seulement en 2017 en ce qui concerne les caméras ANPR, cette exception n'est pas d'application.
[64] *ANPR Managed Services*.
[65] Art. 44/11/3octies de la LFP.
[66] Une analyse *prima facie* implique un contrôle marginal et ne constitue pas un avis formel au sens de l'art 59 LPD.
[67] Ce droit ne figure pas dans le titre 2 de la LPD (traitements policiers). Par ailleurs, l'article 21 du RGPD, dans la mesure pertinente, stipule que le droit d'objection vaut uniquement pour les traitements dans le cadre de l'article 6, 1er alinéa, e) ou f), c'est-à-dire lorsque le traitement n'est pas basé sur une réglementation légale mais est nécessaire à l'exécution d'une mission d'intérêt public ou lorsque les intérêts légitimes du responsable du traitement ou d'un tiers prévalent sur les droits de la personne concernée.
[68] Selon l'article 284 de la LPD, les systèmes de traitement automatisé qui ont été élaborés avant le 6 mai 2016 par les services de police seront conformés à l'article 56 § 1 de la LPD pour le 6 mai 2023 ans plus tard.

données (comme une banque de données technique) qui sont régies après la transformation de la *LED* en LFP[69]. L'Organe de Contrôle répète avec insistance que l'article 56 porte sur les fichiers de journalisation et non sur les droits d'accès aux données.

En ce qui concerne la *DPIA* relative à l'utilisation de la caméra *ANPR* locale, la *DPIA* table à tort sur le fait que des images ne sont pas prises de la plaque d'immatriculation. Un traitement technique (enregistrement) de la photo de la plaque d'immatriculation est incontestablement nécessaire pour pouvoir lire la plaque d'immatriculation et la mettre en corrélation avec les *blacklists*. Par ailleurs, seul un avis du DPO est obligatoire pour utiliser des critères d'évaluation et donc pas la *blacklist* fournie. **L'Organe de Contrôle considère l'implication du DPO dans l'utilisation de listes locales comme une meilleure pratique.**

4.1.8 Registre des images des caméras et des activités de traitement

38. La police n'a pas constitué de registre (séparé) de l'utilisation des caméras. En revanche, l'utilisation des caméras est bien reprise comme une finalité dans le registre local des traitements.
Comme expliqué précédemment, le contenu du registre local des caméras n'est pas encore régi par un arrêté d'exécution. Cela ne doit pas empêcher le chef de corps de constituer de sa propre initiative un registre local (provisoire) de l'utilisation des caméras. Pour des raisons pratiques, le COC peut consentir à reprendre provisoirement l'utilisation des caméras dans une section spécifique du registre des traitements. Il convient dans ce cas de mentionner également les types de caméra (fixes, mobiles, utilisation visible ou non visible) dans cette partie du registre des traitements.

Demande :
Qu'en attendant l'arrêté d'exécution relatif à l'enregistrement local des caméras, le chef de corps constitue un registre local de l'utilisation des caméras ou mentionne clairement dans un volet séparé du registre des traitements les types de caméras, les finalités et le support d'enregistrement des images.

4.1.9. La corrélation des images ANPR avec les listes locales

39. Les images ANPR des caméras ANPR fixes et mobiles sont corrélées à certaines listes objectives. Il s'agit des listes dites « Option 32 »[70], ou des « *blacklists* », et de la liste « Bodoc ». Cette dernière concerne une liste de plaques d'immatriculation internationales en rapport avec des amendes de roulage impayées.

40. Des listes nationales et des listes locales sont utilisées pour les corrélations. En ce qui concerne l'acquisition des listes nationales, ce n'est pas la ZP elle-même mais une autre ZP qui exécute l'option 32[71] nécessaire à cet effet.

---

[69] Voir les articles 44/4 § 2 et 44/11/3novies de la LFP.

[70] L'option 32 donne accès à :
- un fichier des véhicules belges volés et des plaques d'immatriculation (BNG) ;
- un fichier de ces véhicules avec la date des faits (BNG) ;
- un fichier avec des véhicules de la BNG en relation avec une personne qui figure dans la BNG (à l'exception de celles qui sont soumises à un accès limité ou particulier) ;
- un fichier avec des véhicules immatriculés à la DIV (Direction pour l'Immatriculation des Véhicules du SPF Mobilité et Transport) au nom d'une personne connue dans la BNG (à l'exception de celles qui sont soumises à un accès limité ou particulier) ;
- un fichier avec des véhicules belges présumés en défaut d'assurance (Veridass) ;
- un fichier avec des véhicules belges présumés en défaut d'assurance par unité (Veridass) ;
- un fichier avec des véhicules belges en défaut de contrôle technique (GOCA) ;
- un fichier avec des véhicules belges en défaut de contrôle technique par unité (GOCA) ;
- un fichier avec les véhicules néerlandais volés (police néerlandaise) ;
- un fichier avec les véhicules signalés dans SIS II.

[71] L'option 32 est le jargon policier pour l'exécution d'un *téléchargement* de données spécifiques de la BNG à la zone de police qui les demande. L'exécution de cette option est journalisée, de sorte qu'il est possible d'en assurer le suivi par unité. L'option 32 est principalement utilisée pour le téléchargement des données provenant de la BNG (mesures à prendre à l'échelle nationale à l'égard de véhicules et plaques d'immatriculation), du SIS (mesures à prendre à l'échelle internationale à l'égard des véhicules de moins de deux ans), du GOCA (véhicules vraisemblablement en défaut de contrôle technique) et de Veridass (véhicules vraisemblablement en défaut d'assurance). Ces données peuvent être utilisées pour une corrélation dans les banques de données techniques en vue de l'exécution de la politique d'action définie par le groupe de travail police–justice–intérieur qui doit être traduite au niveau de l'arrondissement en une politique d'intervention. L'option 32 contient également des données provenant de la BNG et de la DIV qui permettent d'enrichir les données relatives aux plaques d'immatriculation captées par la caméra ANPR. Pour la BNG, l'enrichissement consiste à savoir si le véhicule ou la plaque d'immatriculation est en corrélation avec une personne connue dans la BNG. Pour la DIV, il s'agit de savoir si le titulaire du véhicule est connu dans la BNG.

L'utilisation de l'option 32 par la ZP n'est donc pas journalisée directement. Cela peut être problématique dans la perspective de la protection des données parce que l'on ne sait donc pas exactement quel service ou entité de police utilise les données téléchargées des sources uniques qui sont à la base des corrélations. Selon la *DPIA* de la caméra *ANPR* mobile, les *blacklists* sont transmises sous forme cryptée par e-mail à la ZP qui les importe ensuite à l'aide d'une clé USB sur l'ordinateur portable de l'ANPR mobile. L'ordinateur portable est un *stand alone* (dispositif autonome) qui n'est pas connecté à Internet[72]. Seuls les numéros d'immatriculation de ces listes obtenues sont retenus, ainsi que le titre de la liste. Les métadonnées fournies (correspondantes) ne sont donc pas utilisées. L'Organe de Contrôle indique que ces données (code du pays, motif(s) du signalement, mesure(s) à prendre et service de police ou pays responsable de ces mesures) sont nécessaires parce qu'elles donnent corps à la politique d'action nationale minimale (fiche opérationnelle C02).

41. Ces listes nationales sont complétées par des listes locales de la ZP. Ces listes locales sont apportées par le service d'intervention et le service d'enquête local **mais les critères d'inscription dans ces listes locales n'ont pu être expliqués.**

Mesure correctrice
Les critères d'inscription sur ces listes locales doivent être expliqués à l'aide de la directive relative à l'interconnexion ou la corrélation de données, d'une part, et à la fiche C02 (du livre 1 de la MFO 3)[73], d'autre part, et transmis à l'Organe de Contrôle dans les 3 mois suivant la notification de cette mesure correctrice.

42. L'exécution des corrélations est effectuée sur un ordinateur portable dans le véhicule de police. **Par conséquent, cet ordinateur portable doit être considéré comme une banque de données technique locale au sens de l'article 44/11/3sexies de la LFP[74].** Comme constaté précédemment, aucune analyse d'impact et de risques n'était du reste disponible pour cette banque de données technique locale. Selon la ZP, seul le dernier *hit* (occurrence positive) est conservé, puis écrasé lorsqu'un *hit* suivant est créé.

En réponse au projet de rapport, la ZP se pose des questions sur le fait que l'ordinateur portable serait considéré pour la caméra *ANPR* mobile comme une banque de données technique. En premier lieu, l'Organe de Contrôle renvoie à l'article 44/11/3*decies* de la LFP qui stipule que la banque de données technique est utilisée pour mettre en corrélation des données à caractère personnel (plaques d'immatriculation) avec des *blacklists* ou avec des critères d'évaluation préalablement déterminés[75]. En deuxième lieu, la *DPIA* soumise à l'Organe de Contrôle s'avère porter à la fois sur l'utilisation des caméras et traitements dans la banque de données, à savoir l'ordinateur portable. À cet effet, la *DPIA* mentionne par ailleurs les articles 44/11/*3sexies à* 44/11/3*decies* inclus de la LFP ; ceux-ci portent sur les banques de données techniques.

43. La réalisation d'un *hit* est mise en relation avec la politique d'action[76] et d'intervention[77]. Le COC a constaté à ce propos que la zone de police ne disposait pas d'une connexion mobile avec des applications de la BNG comme le contrôle de la BNG. Les *hits* sont donc contrôlés par voie radiophonique via le CIC pour vérifier le contrôle de la BNG avant d'intervenir. Ce contrôle peut uniquement être effectué pour les listes de l'option 32 mais pas pour les listes locales. Par conséquent, la politique d'action et d'intervention sur les listes locales manque de clarté, notamment par l'absence des métadonnées nécessaires.

---

[72] *DPIA* caméra *ANPR* mobile, p. 5.
[73] Voir à ce sujet la Directive commune contraignante des Ministres de la Justice et de l'Intérieur *« relative à la détermination des mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou la corrélation des banques de données techniques suite à l'utilisation de caméras ou de systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, visées à l'article 44/2, § 3 de la loi sur la Fonction de Police, avec les banques de données visées à l'article 44/2, §§ 1er et 2 LFP, ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique »*.
[74] Cette banque de données technique locale ne transmet cependant pas de données à la banque de données technique nationale. L'intégration de la caméra (intégration directe) ou de la BTL (intégration par une BTL intermédiaire) doit être demandée auprès du projet ANPR national FedPol DRI BIOPS via le contrat cadre R3 043 Proximus/Trafiroad.
[75] Techniquement, il se fait par ailleurs que la corrélation ne peut, en soi, se dérouler autrement que par le biais d'une base de données technique étant donné que les données provenant des sources uniques qui sont à la base de la corrélation sont traitées dans ces banques de données techniques.
[76] La notion de « politique d'action » renvoie à une combinaison du « Motif du Signalement » (MdS) et de la « Mesure à Prendre » (MàP). Le Motif du Signalement est donc une combinaison de la nature du fait et du critère sur la base duquel l'entité a été corrélée au fait (critère d'enregistrement de base). (P. ex., MdS : volé – vol grave, MàP : saisir). Pour chacune de toutes les combinaisons MdS-MàP possibles théoriquement, une « politique d'action minimale » nationale a été établie par un groupe de travail national police et justice et doit être entreprise si une combinaison déterminée est présente.
[77] La politique d'intervention détermine comment, si, par qui et quand une intervention policière a lieu, à la fois en fonction des accords conclus localement et des possibilités d'intervention au moment même.

Recommandation
En vue d'une application effective et efficace des traitements ANPR, il est important que la ZP élabore une politique claire d'intervention pour les hits sur les listes nationales et une politique claire d'action et d'intervention sur les listes locales.

44. Au regard de la lecture conjointe des autres dispositions de la LFP et de la LPD, l'Organe de Contrôle estime que les listes constituées doivent être évaluées à intervalles réguliers. Il en découle que la liste locale ne peut être conservée pour une « durée indéterminée ». Il faut éviter la formation d'un circuit parallèle de banques de données de police dont les données ne seront pas traitées ou ne peuvent l'être dans les banques de données définies par la LFP.

4.2. Le traitement de données dans la BNG

4.2.1. La gestion fonctionnelle

45. Sur le plan de la gestion fonctionnelle, la ZP collabore avec 2 autres zones de police (province du Limbourg). À cet effet, un pool limité de gestionnaires optionnels permanents collabore avec plusieurs gestionnaires fonctionnels assistants dans lesdites zones de police. Les gestionnaires fonctionnels ont la possibilité de se connecter à distance à leur environnement de travail. C'est favorable pour la rapidité des interventions et cela réduit le nombre de déplacements.

Il s'avère exister à nouveau une bonne collaboration depuis 4 ans avec le SICAD/CIA sur le plan de la huitième fonctionnalité de base de MFO6, à savoir le soutien des gestionnaires fonctionnels du traitement des informations dans les zones de police, notamment par la tenue de réunions de travail trimestrielles avec tous les gestionnaires fonctionnels de l'arrondissement. La ZP y participe activement.

46. Le COC a constaté un bon fonctionnement des flux dirigés sur l'alimentation de la BNG. Préalablement au flux vers la BNG, un contrôle de qualité des données est effectué. Celui-ci est casuistique et n'est pas basé sur des « paramètres de contrôle de qualité » structurels dans l'ISLP. L'option 35[78] est effectuée sur une base quotidienne et nous ne constatons guère de retard dans les refus et les rectifications qui en découlent. Enfin, le gestionnaire fonctionnel n'utilise pas l'option 31[79]. Autrement dit, des comparaisons ne sont pas effectuées en masse entre les données captées par *l'ANPR* et la DIV sur la base de fichiers texte : ce mode de traitement contribue au niveau de protection des données (prévention de fuites massives de données).

47. Pour le moment, la ZP n'a pas de vision des nombres d'entités dont la ZP est l'unité responsable, ni du nombre de fautes possibles par entité identifiée dans la BNG. **Cela se traduit notamment par l'absence d'aperçu du nombre de mesures à prendre pour le moment de sorte qu'un contrôle de qualité sur des critères tels que l'échéance ou la pertinence n'est pas possible**. Cette absence d'aperçu, à son tour, a des implications possibles pour l'exécution correcte de mesures sur le terrain, sous la forme de corrélations par l'intermédiaire du fonctionnement ANPR. Dans l'intérêt d'un contrôle de qualité structurel de la BNG relatif aux entités dont la ZP est l'unité responsable, la ZP est demandeuse de la mise à disposition d'un tableau de bord clair qui indique, par paramètre, les quantités ainsi que les clés techniques à des fins de contrôle.

48. Néanmoins, le COC a constaté que la ZP utilisait une vision qui est clairement conforme à la direction MFO3 et au « vade-mecum de la police judiciaire ». Dès lors, on n'utilise pas un PV (procès-verbal) avec code de parquet 45 pour les actions suspectes mais bien le concept du RIR[80]. Le critère d'enregistrement de base « élément d'enquête » n'est pas utilisé non plus pour la corrélation entre entités et faits concrets. La vision relative aux corrélations entre entités et enquêtes correspond complètement à la logique à ce sujet : plus de corrélation entre entités et une enquête clôturée à moins que la corrélation puisse être établie par un fait concret.

[78] L'option 35 est le jargon politique pour l'exécution du flux des banques de données de base vers la BNG.
[79] L'option 31 est le jargon de la police pour l'exécution d'une consultation générale de la DIV sur la base d'une liste de captations d'une banque de données technique ANPR qui a été obtenue à l'aide d'une *query* (recherche).
[80] Les « actes suspects » sont des données en réalité douces (non concrètes) qui reçoivent le statut impropre de données concrètes avec le délai de conservation correspondant en les traitant à la manière d'un code de parquet PV 45 "Actes suspects" dans la BNG.

49. Le COC a constaté aussi au sein de la ZP une inquiétude quant à la qualité des données provenant d'une autre banque de données[81]; des problèmes seraient identifiés quant à l'exactitude des noms, des prénoms, des dates de naissance et de la nationalité. Le COC estime également pouvoir détecter une certaine inquiétude à partir d'une question explicite de l'Organe de Contrôle relative à l'utilisation d'une banque de données citée nommément spécifique. L'Organe de Contrôle présume donc que l'utilisation de cette banque de données et les processus qui en découlent pourraient avoir une influence négative sur la relation correcte des enquêtes dans la BNG de telle sorte que la coordination des enquêtes est compliquée dans le fonctionnement SICAD/CIA. Le COC s'informera propos de ces traitements et entamera une enquête.

50. Une vision claire est présente quant aux consultations de la BNG. Le profil FNC[82] est réservé aux membres des services locaux de recherche (SLR) et aux membres de la gestion fonctionnelle. Plusieurs inspecteurs principaux des autres services disposent également de ce profil mais ont reçu une formation claire à cet effet. Selon la ZP, on s'efforce également de compléter un motif clair de consultation[83]. Certes, la zone de police n'a pas produit de documents politiques en la matière. Il est seulement fait référence à une instruction récente du chef de corps[84]. Pendant la visite sur place, le COC n'a pas procédé à un coup de sonde sur ce plan.

51. Pour les contrôles sur le terrain, on se base en premier ressort sur le « contrôle de la BNG » pour analyser les mesures à prendre. Il a pu être constaté que la police faisait clairement preuve de connaissances sur la façon dont il vaut mieux procéder à une consultation dans la BNG. Enfin, la zone de police utilise les outils opérationnels disponibles.

52. Il ressort de ce qui précède que la ZP possède de bonnes connaissances et vision sur le plan du fonctionnement de la BNG et qu'un tableau de bord BNG tel que celui envisagé par le COC serait un bon auxiliaire.

53. Des contrôles proactifs (périodiques) des consultations illicites éventuelles ne sont cependant pas effectués. L'Organe de Contrôle souligne qu'outre la LPD, une circulaire du procureur du Roi de Flandre orientale prescrit par exemple expressément des contrôles proactifs de la licéité des traitements dans les banques de données policières depuis le 15 décembre 2017 (cf. OBOV 2017-016 du 7 septembre 2017 relatif aux « *Basisrichtlijnen inzake het consulteren van databanken* » (Directives de base relatives à la consultation de banques de données)) : « *Binnen de onderscheiden politiediensten dienen er regelmatig (minstens halfjaarlijks) steekproefsgewijze controles te gebeuren op het rechtmatig gebruik van de databanken. Vastgestelde inbreuken op het beheer, toegang en gebruik van de databanken moeten onverwijld aan het openbaar ministerie worden gemeld. Inbreuken kunnen aanleiding geven tot strafrechtelijke en/of tuchtrechtelijke vervolging*" (p. 3) (traduction libre : Dans les différents services de police, il faut procéder régulièrement (au moins chaque semestre) à des contrôles par coups de sonde de l'utilisation licite des banques de données. Les infractions constatées à la gestion, l'accès et l'utilisation des banques de données doivent être communiquées sans retard au ministère public. Les infractions peuvent donner lieu à des poursuites pénales et/ou disciplinaires).

Eu égard au manquement constaté, l'Organe de Contrôle insiste pour l'élaboration d'une policy/politique qui prévoit un mécanisme d'exécution périodique et effective de contrôle de la surveillance des éventuelles consultations illicites notamment en vertu de la LPD et ce par analogie à une obligation imposée par le procureur du roi de Flandre orientale et aux bonnes pratiques.

Mesure correctrice
Consulter régulièrement les journalisations de la BNG et effectuer des contrôles proactifs par coups de sonde (2 x/an) dans le but de surveiller l'introduction obligatoire d'un motif de consultation et les consultations irrégulières éventuelles et ce une première fois dans les six mois qui suivent la notification de cette mesure correctrice et d'en mettre leurs résultats à la disposition du COC.

[81] Il s'agit d'une nouvelle plate-forme numérique de communication et d'information pour le suivi de personnes libérées sous conditions.
[82] Pour les consultations de la BNG Consultation, une distinction est opérée entre l'exploitation de base du profil (information associée à des faits concrets) et l'exploitation avancée (information associée à des faits non concrets et enquêtes). L'utilisation de ce dernier profil implique ue connaissance approfondie des concepts utilisés dans la BNG afin de pouvoir donner une interprétation correcte des résultats d'une consultation. Les zones de police sont responsables de la gestion et du contrôle des accès à la BNG dont disposent les membres du personnel relevant de leur responsabilité. Le profil FNC (« fait non concret ») permet d'obtenir plus d'informations mais une utilisation non correcte sur le terrain peut occasionner des dommages aux enquêtes en cours.
[83] Il s'agit d'un e-mail du chef de corps du 1er septembre 2020 au personnel de la police en prévision de la visite du COC.
[84] Il s'agit d'un e-mail du chef de corps du 1er septembre 2020 au personnel de la police en prévision de la visite du COC.

4.2.2. La validation des données (validation centrale)

54. Les données enregistrées structurées doivent, après préparation dans l'application locale (ISLP[85], saisie locale…), être transmises au niveau central où elles sont automatiquement contrôlées.

La ZP a procédé à 61 transferts de données au total entre le 01/01/2020 et le 31/03/2020 $(Option 35). Cela signifie que des données enregistrées localement sont transmises chaque jour ouvrable au niveau central : c'est une **constatation positive** étant donné qu'elle assure une alimentation continue vers le niveau central.

4.3. Banques de données particulières

55. Avant l'introduction de la loi de 2019 relative à la gestion de l'information policière 2019[86], Il existait une obligation expresse de déclaration des banques de données particulières auprès de l'Organe de Contrôle. Depuis l'entrée en vigueur de cette loi, les banques de données particulières doivent être reprises dans le registre des traitements (voir la rubrique 3.3.9)[87]. L'Organe de Contrôle constate qu'une série de banques de données particulières sont reprises dans le registre. La ZP ne dispose cependant pas d'un ordre de corps dans lequel sont définies les circonstances et les conditions à la constitution et à l'utilisation d'une banque de données particulière.

56. Sans soumettre toutes les banques de données particulières mentionnées dans le registre à un contrôle de leur contenu, le COC estime que plusieurs des activités de traitement relèvent difficilement d'une banque de données particulière. Citons comme exemple l'enregistrement des données suivantes : un registre des événements, des demandes dans le cadre de la gestion des accès aux banques de données policières et une banque de données particulière pour les « dossiers COVID-19 ». Conserver ces derniers dans une banque de données particulière est particulièrement étrange parce qu'un module séparé est prévu dans le BNG pour le traitement de ces procès-verbaux. Le traitement de ces données dans une banque de données particulières est par conséquent contraire aux dispositions relatives à la gestion des informations prévues dans la LFP.

En réponse à une remarque de la ZP sur le projet de rapport, l'Organe de Contrôle fait remarquer que les traitements non opérationnels ne relèvent pas de l'application de la LFP mais bien du RGPD, comme les données à caractère personnel. En ce qui concerne les dossiers « COVID-19 », l'Organe de Contrôle constate que les traitements policiers dans ce cadre doivent se dérouler à l'aide des processus de traitement réguliers. L'Organe de Contrôle se demande donc ce qu'il faudrait encore traiter en plus sous le dénominateur de la banque de données particulière « COVID ».

Recommandation
Le COC insiste pour que la ZP définisse dans une note de corps une politique pour la constitution de banques de données particulières reprenant les paramètres sur la base desquels s'opère le contrôle de la conformité de la constitution d'une banque de données particulière pour cette activité de traitement déterminée aux conditions légales de l'article 44/11/3 de la LFP.

4.4. L'utilisation d'appareils mobiles dans le cadre ou non de missions opérationnelles et l'utilisation d'images caméra à des fins non opérationnelles

57. À ce propos, les cas suivants ont été soumis à la ZP :

1) L'utilisation d'un smartphone pour procéder à des constatations en cas d'accident grave de la route ou d'effraction ;
2) Le service ICT signale au chef de corps une consommation excessive inexplicable de données par le personnel de la police. Quelle est la procédure appliquée ?
3) Un citoyen prétend qu'il n'a pas été reçu correctement à l'accueil par le fonctionnaire de la police. Des caméras fixes sont utilisées à l'accueil.

[85] *Integrated System for the Local Police*.
[86] Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *M.B.* du 19 juin 2019.
[87] Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière. Art. 44/11/3 de la LFP WPA *juncto* l'article 145 de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.

58. La zone de police répond à propos de l'utilisation d'appareils privés pour des traitements opérationnels que l'utilisation d'appareils privés en cas d'interventions n'est pas autorisée. Ce cas ne se serait pas encore produit. Selon la zone de police, les appareils professionnels nécessaires sont mis à la disposition du fonctionnaire de la police.

59. À ce propos, la ZP dispose de deux ordres de corps qui portent respectivement sur la « *sécurité générale des informations* » du 14 août 2020 et « *Policy Mobile Devices/FOCUS – réglementation pour l'octroi de smartphones et d'abonnements* » du 11 septembre 2020[88]. **L'ordre de corps « sécurité générale des informations » n'offre cependant pas une réponse (satisfaisante)** aux premier et deuxième cas hormis le fait que la ZP met à la disposition du personnel un appareil de service ou d'entreprise et, en 2020, il faut obligatoirement procéder à l'utilisation de l'appli Focus qui permet de *« transmettre des images et suivre des incidents »*. Le membre du personnel peut toutefois choisir d'utiliser son propre arrêt mais l'appli Focus doit également être installée sur l'appareil personnel.

60. Dans l'ordre de corps « *Sécurité générale des informations* », une rubrique est consacrée à l'« Utilisation de services Internet commerciaux et de clouds publics[89]. Il y est spécifié que « *de politiemedewerkers* (*kunnen*) *tijdens de uitoefening van hun taken geen gebruik maken van commerciële internetdiensten en publieke clouds zoals Whatsapp, Facebook (…) met uitzondering van nooddiensten* » (Traduction libre : les collaborateurs de la police ne peuvent, pendant l'exercice de leurs tâches, faire usage des services Internet commerciaux et de clouds publics tels que WhatsApp, Facebook (…), à l'exception des services d'urgence »), parce que ces services n'offrent pas de garanties suffisantes que le RGPD[90] soit respecté. Ensuite, une rubrique est consacrée brièvement à "*Externe communicatie, internetpatrouille en onlinerecherche*" (Communication externe, patrouille Internet et recherche en ligne »). Il y est stipulé que : « *De geïntegreerde politie kan nog wel gebruik maken van allerlei commerciële internetdiensten voor doeleinden waarbij wij als organisatie geen persoonsgevens verwerken* [91]*. Enkele voorbeelden hiervan zijn:*
- Externe communicatie via korpsprofiel op bijvoorbeeld Facebook of Twitter.
- Gebruik van profielen op sociale media in het kader van internetpatrouille of recherche »[92] (traduction libre : La police intégrée peut utiliser toutes sortes de services Internet commerciaux pour des finalités pour lesquelles nous ne traitons pas de données à caractère personnel en tant qu'organisation Quelques exemples sont : - communication externe via le profil du corps, par exemple sur Facebook ou Twitter.- utilisation de profils sur des réseaux sociaux dans le cadre de patrouilles Internet ou de recherches).

61. Avant tout, la lecture conjointe avec la rubrique précédente révèle un manque de clarté pour le fonctionnaire de police (et pour le COC) ou du moins des propos qui prêtent à confusion, quant aux cas dans lesquels le fonctionnaire de police peut ou non utiliser les réseaux sociaux alors que des informations et données à caractère personnel sont traitées avec un caractère opérationnel. Ensuite, il n'est évidemment pas exact que la police ne traiterait pas de données à caractère personnel lorsqu'elle participe à des réseaux sociaux[93].

62. En ce qui concerne le contrôle de la consommation excessive de données (2e cas), les réponses révèlent que **la ZP suit une procédure qui est le reflet ou une application analogue des principes de la convention collective de travail (CCT) numéro 81 relatifs au contrôle de l'utilisation d'Internet**[94]**.** Cette CCT est obligatoire de telle sorte qu'elle s'applique à tous les employeurs dans le secteur privé et n'est donc pas d'application au service public, comme la GPI. Cette CCT n° 81 contient toutefois les principes de base du droit relatif à la protection des données à caractère personnel (RGPD) de sorte que rien n'empêche que la police adhère aux conditions de base de cette CCT n° 81 ou les applique par analogie pour l'introduction de contrôles sur le lieu de travail. Il en va de même pour le troisième cas, les images des caméras qui sont utilisées initialement à des fins policières (LFP) peuvent également être utilisées dans le contexte du droit du travail (finalité RGPD). **Pour le COC, cette attitude constitue tout simplement une *meilleure pratique*.**

[88] Ordre de Service n° 12/2018.
[89] Rubrique 7, p. 13.
[90] Règlement général pour la Protection des Données ou RGPD.
[91] Soulignement COC.
[92] Rubrique 7.2., p. 14.
[93] Par ailleurs, il n'est pas exclu dans tous les cas que l'utilisateur doive également être considéré comme un responsable du traitement (conjoint) (voir CJCE, 29 juillet 2019, Fashion ID, C-40/17).
[94] CCT n° 81 Convention collective de Travail n° 81 du 26 avril 2002 conclue au sein du Conseil National du Travail « relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau ».

63. Il est toutefois important que la ZP élabore dans un ordre de corps la procédure énonçant concrètement les principes de base de manière transparente : finalités, nécessité et proportionnalité, conséquences pour la personne concernée et les droits de la personne concernée[95]. L'utilisation de données policières dans la relation de travail induit l'application du RGPD à ce traitement ultérieur (transparence et droits de la personne concernée). Il en va de même en ce qui concerne l'utilisation des images de caméras opérationnelles pour le contrôle du respect des conditions de travail. À ce propos, l'Organe de Contrôle renvoie à son Avis d'initiative du 17 août 2020 concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail (BD20007), qui peut servir de fil conducteur[96].

Recommandation
Il importe que le chef de corps opère, dans l'ordre du corps, une distinction claire entre les divers aspects visés sur le plan de l'accès et de l'utilisation d'Internet et des réseaux sociaux pour des objectifs personnels et professionnels et de l'utilisation ou non d'appareils personnels[97]. C'est ainsi que l'accès à Internet (recherches, sites autorisés et interdits) pendant les heures de service doit être distingué de l'utilisation des réseaux sociaux pendant les heures de service à des fins personnelles, d'une part, et dans la mesure où des informations policières pourraient être partagées, d'autre part. Dans un volet séparé ou un document distinct, l'utilisation d'appareils mobiles privés à des fins opérationnelles et l'utilisation d'appareils mobiles professionnels à des fins personnelles doivent être décrites (séparément). En l'occurrence, il importe que le document décrive clairement ce qui est autorisé et interdit, dans quelles circonstances et à quelles conditions un contrôle peut être effectué, quelles sont les conséquences de la constatation d'infractions au document et les droits de la personne concernée dans ce cadre. Il est donc primordial d'opérer une distinction claire entre les divers aspects et finalités en élaborant une procédure qui définit concrètement les principes de base de la transparence et les droits de la personne concernée. C'est également le cas en ce qui concerne l'utilisation d'images de caméras opérationnelles pour le contrôle du respect des conditions de travail.

4.5. Protection des données

4.5.1. Le traitement de données biométriques à des fins non opérationnelles

64. En vue du pointage des membres du personnel[98] et du contrôle d'accès, la ZP n'utilise pas d'empreintes. Sur le plan de l'utilisation d'appareils mobiles, l'ordre de corps *Mobile Devices*, rubrique 4.1.1. « Mot de passe » (page 12) stipule comme suit : « *Zowel voor de dienst- en bedrijfstoestellen als voor de privétoestellen (BYOD) dient de ontgrendelingsmethode met biometrie te gebeuren indien het toestel deze mogelijkheid biedt. Er dient een sterk wachtwoord ingesteld te worden als back-up of als biometrisch ontgrendelen niet mogelijk is » (*Tant pour les appareils de service et d'entreprise que pour les appareils privés (BYOD), la méthode de déverrouillage biométrique doit être utilisée si l'appareil offre cette possibilité. Un mot de passe fort doit être paramétré en solution de secours ou si le déverrouillage biométrique n'est pas possible). Selon la ZP, il ne s'agit cependant pas d'une obligation et l'application d'un déverrouillage biométrique des appareils de service et d'entreprise ne peut être contrôlée par la ZP. Le COC renvoie aux incohérences remarquées précédemment à ce sujet (voir les numéros 60 et 61) dans les ordres de corps et leur application pratique.

65. Par souci d'exhaustivité, le COC fournit des explications à propos de la raison de cette demande aux zones de police et du point de vue du COC. L'enregistrement de l'utilisateur dans le système est effectué par la collecte des caractéristiques biométriques pertinentes de cette personne qui sont associées aux données auprès du service du personnel. La raison principale[99] pour introduire le système de contrôle concerne l'aspect de l'authentification, à savoir que celui qui s'inscrit est effectivement la personne à laquelle les données d'identification correspondent. Bien que le principe de départ soit en général que tous les membres du personnel utilisent leurs empreintes digitales pour le pointage, il est néanmoins possible d'utiliser – en guise d'alternative – un badge personnel.

[95] En ce qui concerne la surveillance par caméras, voir l'avis d'initiative du COC « concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail » (BD200007), https://www.organedeContrôle.be/files/BD200007_Surveillance_Camera_Lieu_de_Travail_Avis_dOffice_17-08-2020_00016316.PDF.
[96] www.Contrôlergaan.be/publicaties/adviezen/aanbevelingen.
[97] L'Organe de Contrôle attire l'attention en l'occurrence sur les réglementations légales qui protègent la confidentialité de la communication privée, comme l'article 314bis du Code pénal et la loi du 13 juin 2005 « *relative aux communications électroniques* » qui protège la confidentialité des télécommunications (article 5 de cette loi).
[98] Tant les fonctionnaires de police que le personnel du CALog.
[99] Le gain d'efficacité sur le plan de l'administration du personnel est évoqué également.

66. Le système fonctionne comme suit. Pour déterminer les données de la personne concernée dans le système, une image de l'empreinte digitale est d'abord générée. Un algorithme spécial convertit les empreintes digitales en un code unique qui est ensuite enregistré dans un *Record*, le *template*. La lecture des caractéristiques biométriques de la personne concernée est effectuée par une comparaison des empreintes digitales avec les données enregistrées (*matching)* sur le *template.* Bien que les empreintes ne soient pas enregistrées telles quelles, les données biométriques sont converties en un code unique sur la base duquel la personne concernée est identifiée (un système central du service du personnel). **Ce code unique contient donc la traduction chiffrée des empreintes qui concernent incontestablement les données biométriques à caractère personnel de la personne concernée. Que ces empreintes soient conservées « en clair » ou en « *template* » ou « modèle » (ce code unique) ne fait pas de différence : ces données sont et restent des données biométriques.**

4.5.2. Le consentement

67. Le consentement en tant que base juridique (art. 9.2 a) RGPD) n'est pas acceptable étant donné le lien de subordination et la relation de pouvoir. **En l'espèce, le consentement d'un membre du personnel de la police intégrée n'est jamais vraiment « libre » au sens du droit relatif à la protection des données.** Même lorsqu'une alternative est proposée (comme c'est le cas en l'espèce du numéro de matricule enregistré dans le badge), le consentement comme fondement légal du traitement des empreintes numériques reste caduc.

4.5.3. Intérêt public important

68. Citons encore comme base légale l'art. 9.2 g) du RPGD qui autorise le traitement de données biométriques si *« le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »*. **Une telle disposition en droit interne ou base juridique n'est pas présente en Belgique**.

4.5.4. Obligations du responsable du traitement (le chef de corps)

69. L'article 9.2 b) du RGPD semble offrir une dernière option, à savoir que le traitement *« est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée »*. **Cette fois encore, une telle disposition en droit interne ou base juridique n'est pas présente en Belgique**. Une convention collective de travail n'est pas une possibilité non plus étant donné que nous nous trouvons dans le secteur public. En d'autres termes, même s'il y avait un accord collectif avec le personnel (syndicat), celui-ci ne constituerait pas une base juridique suffisante parce qu'en droit belge, un accord avec les syndicats dans le secteur de la police n'est pas une norme juridique contraignante. Quoi qu'il en soit, une telle convention collective devrait de toute façon offrir « *des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée* ».

Le COC a également obtenu l'avis sur ce plan de la police fédérale, direction générale de la gestion des ressources et de l'information (DGR). La vision de cette direction est présentée littéralement ci-dessous avec le passage mentionné en gras qui en traduit l'essence même selon le point de vue du COC et atteste que la DGR se rallie également à la vision du COC.
"Faisant suite à votre mail du 28 mars 2019, vous trouverez ci-après la position du service juridique de la police fédérale. Cette position a été concertée avec les différentes entités en charge de l'interprétation et de l'application de la réglementation en matière de protection des données.
L'article 9.2 b) du RGPD exige qu'un traitement de données considérées comme sensibles soit autorisé « par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ».

Le statut syndical (réf. 2) pose le principe de la négociation préalable avec les organisations syndicales représentatives lors de l'adoption de réglementations de base ayant trait au statut policier, et érige par ailleurs le comité de négociation en organe d'avis des ministres de tutelle. Il s'agit, pour l'autorité, de consulter et d'informer les représentants des membres du personnel de ses intentions. La négociation constitue donc une "étape de procédure" dans l'adoption de textes légaux et réglementaires statutaires.
Le protocole qui résulte des négociations syndicales ne crée pas une « règle de droit » contenant des droits et obligations pour les membres du personnel et ne constitue par conséquent pas, en lui-même, un fondement suffisant au sens de l'article 9.2 b) du RGPD. A l'instar des conventions collectives dans le secteur privé, lesquelles sont rendues obligatoires par arrêté royal, un accord syndical doit, selon nous, être formalisé dans un instrument légal ou réglementaire afin de répondre aux exigences du règlement européen.
Pour votre information complète, une vision intégrée concernant l'utilisation des empreintes digitales dans le cadre de l'application du statut est en cours de réflexion au sein de la police intégrée, afin d'uniformiser les pratiques en la matière. Cette vision intégrée ne fera pas l'économie d'une analyse de la subsidiarité et de la proportionnalité d'un tel traitement de données à caractère personnel au regard des finalités poursuivies, tandis que les garanties appropriées devront être déterminées ».

71. À l'instar de l'analyse précédente, l'Organe de Contrôle estime, pour autant que nécessaire, qu'un rapport du GSN et/ou l'avis de l'APD peuvent difficilement être considérés comme une base juridique. Ainsi le rapport du GSN ne fait-il en aucune manière allusion au fait qu'un système de contrôle avec des empreintes digitales serait introduit, moins encore qu'une base légale serait désignée. En ce qui concerne l'avis de l'APD, il faut souligner que celui-ci a été rendu en 2008, en application de la loi du 8 décembre 1992 relative au traitement de données à caractère personnel, abrogée entre-temps, dans laquelle le traitement des données biométriques n'était pas régi. Par ailleurs, quand bien même on pourrait tenir compte de l'avis - quod non -, l'APD estime que l'introduction du système n'est admissible que dans des cas exceptionnels. Aucune autre mesure prêtant moins à conséquence pour la vie privée ne pourrait conduire au même résultat et il doit s'agir de lieux présentant un risque (élevé) particulier pour la sécurité. La possibilité offerte de s'inscrire quand même à l'aide du badge personnel atteste à elle seule que le traitement des empreintes digitales par la ZP n'est pas pertinent.

72. Les informations qui précèdent amènent enfin l'Organe de Contrôle à la conclusion qu'un système d'empreintes digitales du personnel n'est **pas légal** pour la finalité indiquée *de lege lata*.

4.5.5. Le registre de traitements

73. La ZP possède un registre de traitements.

4.6 Délégué à la protection des données (DPO)

74. La zone de police fait appel à une déléguée à la protection des données (DPO) désignée au niveau provincial (binôme)[100] et à un assistant *DPO* qui est désigné au niveau du corps. Les deux appartiennent au cadre administratif (membre du personnel CALog). La DPO provinciale exerce sa fonction de DPO à temps plein mais travaille en cette qualité pour plusieurs zones de police, donc aussi la PZI[101]. La *DPO* provinciale répond toutefois de la coordination de pas moins de 14 zones de police dont 6 zones de police disposent d'un assistant *DPO*. Dans la ZP, la *DPO* est donc assistée par une personne de contact locale.

75. Bien qu'un *DPO* puisse effectivement être désigné pour différentes zones de police, il faut veiller à ce que celui-ci puisse exécuter ses missions de manière effective et efficace. Un DPO doit disposer de temps et de moyens suffisants pour pouvoir exercer sa fonction. La notion de *« temps disponible suffisant »* n'est définie nulle part. Le DPO devra donc l'apprécier en fonction de chaque situation étant entendu qu'il doit pouvoir effectivement s'acquitter de sa tâche. La fonction du DPO n'est donc pas nécessairement un emploi à temps plein. Dans ce cadre, le DPO doit pouvoir disposer des informations dont il a besoin pour l'exécution de ses tâches et, à cet effet, il a accès aux différents canaux d'information et organes décisionnels au sein de la zone de police pour l'impliquer le plus étroitement possible dans les activités de la zone de police. Étant donné le caractère multidisciplinaire de la protection des données et de la sécurité

[100] Art. 144 de la loi sur la police intégrée et articles 63, 64 et 65 de la LPD
[101] Comme prévu à l'article 144, 2e alinéa de la loi sur la police intégrée.

des informations et l'expertise et les compétences très spécifiques dont un DPO doit disposer, l'Organe de Contrôle est parfaitement conscient que ce n'est pas une tâche évidente pour une zone de police de toujours désigner au sein de sa propre organisation un candidat adéquat pour assumer cette fonction (allant d'un nombre limité d'heures par semaine/temps partiel à un temps plein éventuel) et de prévoir également les moyens nécessaires (temps/argent) à cet effet pour lui permettre de développer et d'entretenir son expertise

76. L'Organe de Contrôle a constaté que la ZP faisait appel à une DPO qui dispose des compétences requises et exerce à temps plein ses fonctions, réparties sur plusieurs zones de police. Au total, il s'agit ici de quatorze (14) zones de police. Le nombre d'heures par semaine (ou exprimées en pourcentage ETP) que la DPO consacre à sa fonction de DPO coordinateur pour la ZP n'est pas arrêté. La DPO a argumenté que son emploi du temps par corps était impossible à déterminer ; elle répartit au mieux le temps disponible entre les différentes zones de police. Ce faisant, elle peut consacrer toute son attention à cette matière et ainsi continuer à étendre et entretenir son expertise et ses connaissances (pratiques) dans le domaine de la protection des données.

77. Une même personne peut donc certes fournir des services à plusieurs zones de police mais le nombre d'heures par semaine qu'elle consacre effectivement en tant que DPO pour une zone de police doit naturellement être réaliste pour pouvoir exécuter dûment sa fonction. L'Organe de Contrôle estime qu'un DPO doit pouvoir opérer au moins 4 heures par semaine en cette qualité pour la même zone de police à moins qu'il soit possible de démontrer à suffisance par rapport à l'organe de contrôle que cela n'est ou ne serait pas nécessaire. Le nombre total d'heures par semaine (la somme du nombre d'heures par semaine dans chaque zone de police concernée) ne peut en aucun cas dépasser quarante (temps de travail prévu pour 1 ETP). Étant donné l'ampleur de sa fonction de coordination (14 ZP dont 6 ont aussi leur propre assistant), il semble très douteux que la DPO puisse consacrer un temps suffisant à ses missions légales pour la ZP.

Contrairement à ce que la ZP estime devoir déduire dans la réponse au projet de rapport du numéro précédent, il s'agit d'une *moyenne* d'au moins quatre heures par semaine, *répartie* sur toutes les activités ou tâches que la DPO exerce dans sa zone de police.

78. À partir des réponses au questionnaire envoyé, des interviews réalisés pendant la visite du place et de la liste actuelle des actions restant à entreprendre en matière de protection des données (poursuite de l'élaboration, actualisation et mise en œuvre d'une politique en matière de protection et de sécurité des informations, exécution de *DPIA*, engagement continu à la sensibilisation), **l'Organe de Contrôle parvient à la constatation que la DPO coordinatrice pour la ZP, étant donné son budget-temps limité, est plutôt, à la demande spécifique de la ZP sur le fond, impliquée dans la mise en œuvre, la gestion quotidienne et le suivi de la politique en matière de protection des données et de sécurité des informations**, ce qui augmente le risque qu'elle ne puisse pas, ou pas à temps, rendre des avis à propos des activités de traitement des données et assumer pleinement son rôle. La DPO intervient plutôt comme expert (notamment, établissement de modèles de documents, communication de méthodologies, etc.) et comme coach pour la personne de contact interne/le coordinateur de la protection des données.

79. **L'Organe de Contrôle n'a par conséquent pas pu constater que la DPO suivait ou pouvait suivre de manière suffisante les activités de traitement de la police afin de vérifier leur conformité avec la législation en matière de protection des données**. En effet, la DPO doit également être impliquée proactivement dans toutes les matières relatives au traitement des données, cela nécessite également un rôle plus actif de la direction.

Recommandation
L'Organe de Contrôle insiste sur une rectification du budget-temps pour la DPO et sur la limitation du nombre de zones de police pour lesquelles elle exerce un rôle coordinateur en tant que DPO. Le COC estime que, dans les circonstances actuelles, la DPO ne peut pas disposer de moyens suffisants (temps) pour exécuter correctement les tâches de DPO pour le grand nombre de zones de police.

Dans la ZP, un accord de coopération officiel a été mis en place entre différentes zones de police, initiative qu'il faut saluer. Cela ne pourrait en principe que favoriser la cohérence et l'efficacité de la politique en matière de protection des données. Mais, même dans le cadre d'un accord de coopération, la ZP doit faire en sorte de prévoir que des moyens suffisants soient débloqués pour que les tâches du DPO puissent être exécutées correctement. La mise en

œuvre pratique est un choix du responsable du traitement. Le DPO peut être soutenu par une équipe pour exécuter l'ensemble de ses tâches. Le DPO et son équipe tiennent lieu de point de contact au sein de la ZP pour toutes les questions relatives au respect de la législation en matière de protection des données et doivent donc être impliqués étroitement dans les activités de traitement de la zone de police.

Ajoutons à cela que le COC estime que, même si une ou plusieurs personnes de contact locales sont désignées et formées au sein de la ZP concernée en vue de soutenir le DPO pour la coordination pratique, le suivi et la mise en œuvre de la politique et des processus en matière de protection des données et de sécurité des informations, un budget-temps (très) limité pour un DPO (c'est-à-dire un nombre limité d'heures par semaine) ne peut être praticable/faisable que moyennant plusieurs conditions préalables, à savoir :

- le *DPO* peut dûment exécuter ses attributions légales (article 39 du RGPD et article 65 de la LPD). Elles se composent donc comme suit :
    - informer et conseiller sur tous les aspects de la protection des données ;
        - en particulier en ce qui concerne les évaluations de l'impact sur la protection des données et de l'établissement du registre des informations de traitement
        - en particulier en ce qui concerne les éventuelles *data breaches ;*
    - contrôler le respect de la législation en matière de protection des données (RPGD, LPD, LFP) et des règles internes en matière de protection des données ;
    - faire office de point de contact pour l'autorité de contrôle et collaborer avec elle ;
    - faire office de personne de contact pour la zone de police sur les questions relatives au traitement de données (y compris la sécurité des informations), tant des collaborateurs internes que des personnes concernées externes.
- Une certaine sensibilisation est déjà présente dans toutes les couches de l'organisation sur l'importance d'une politique adéquate de protection des données ;
- le *DPO* est impliqué activement dans les activités de la ZP et informé de toutes les activités de traitement des données afin qu'il puisse donner à temps les avis nécessaires.

En réponse au projet de rapport, la ZP fait remarquer que l'assistance lors de l'établissement du registre des activités de traitement n'est pas une obligation légale (article 39 du RGPD et 65 de la LPD). L'Organe de Contrôle fait remarquer que l'assistance et l'avis du DPO sont en rapport avec le traitement des données à caractère personnel, quelle que soit la personne (fonction/profil) qui doit établir et actualiser le registre des traitements.

4.7 Sécurité de l'information

4.7.1. Politique et organisation

81. En ce qui concerne l'élaboration de la politique en matière de sécurité des informations et de protection des données, l'Organe de Contrôle est conscient que la « politique » est un concept vaste qui pourrait être concrétisé dans un règlement d'ordre intérieur ou un ou plusieurs ordres de service.

La ZP dispose à cet égard des documents de base suivants :

- Ordre de Corps- Algemene informatieveiligheid (date de promulgation : 31 janvier 2019) ;
- Ordre de Corps - Korpsgewoontes voor de informatieveiligheid (date de promulgation : 14 août 2020) ;
- Ordre de Corps - Omgaan met politionele informatie en databanken (date de promulgation : 31 janvier 2019) ;
- Ordre de Corps - Policy Telewerken (date de promulgation : 11 septembre 2020) ;
- Ordre de Corps - Gebruik van *Office 365* GPI en *Sharepoint* (date de promulgation : 31 janvier 2019) ;
- Ordre de Corps - *Policy Mobile Devices*/FOCUS – regeling voor toekenning en gebruik van *smartphones* en abonnementen (date de promulgation : 11 septembre 2020).

82. L'ordre de corps "*Algemene Informatieveiligheid*" (Sécurité générale des informations) peut être considéré comme la politique de corps en matière de sécurité des informations : il décrit notamment les rôles et responsabilités de tous

les collaborateurs et dirigeants en matière de sécurité des informations, la désignation d'un DPO, un modèle de classification des données (publiques, internes, limitées) et plusieurs directives et procédures à respecter. Ce document politique renvoie pour plusieurs thèmes spécifiques à des directives de corps distinctes (par exemple, la note de corps *« Omgaan met politionele informatie en databanken »* (gestion des informations policières et banques de données). Nous avons constaté que la note de corps mentionnée « *Omgaan met ICT-middelen »* (gestion des moyens ICT) était encore en préparation.

Comme indiqué précédemment, le COC a constaté certaines divergences entre les documents. Cela tient en grande partie à la généralité des documents en ce sens qu'ils ne sont pas parfaitement adaptés à l'organisation spécifique de la zone de police.

83. La Politique de sécurité des informations n'a pas encore été concrétisée en un plan de sécurité des informations approuvé par le chef de corps[102]. Les mesures de la maturité et/ou les analyses de risque formelles relatives à la sécurité des informations et à la protection des données ne sont pas effectuées sur une base périodique. Le COC n'a pas pu déterminer d'approche formelle pour l'évaluation et la maîtrise des risques relatifs à la sécurité des informations et, en particulier, des informations à caractère personnel.

84. En application de l'arrêté d'exécution du 6 décembre 2015, la ZP devait déjà disposer d'un plan de sécurité des informations. Il s'agit donc ici d'élaborer, de suivre et de mettre à jour régulièrement un plan de sécurité des informations contenant les priorités, le ou les responsables et les délais pour la réalisation des mesures proposées du plan. Ce plan est revu régulièrement sur la base des décisions de la direction, de nouveaux risques, de la législation modifiée et d'autres tâches organisationnelles.

Mesure correctrice
La ZP doit établir un plan de sécurité des informations. Le plan de sécurité des informations sera mis à la disposition de l'Organe de Contrôle dans les six mois suivant la date de la notification du présent rapport à l'Organe de Contrôle

Recommandation
Il est recommandé de reprendre les points d'action suivants dans le plan de sécurité des informations :

- *la poursuite de l'élaboration et l'affinement de la politique en matière de sécurité des informations et de protection des données par le biais de directives du corps et de procédures. Cette politique doit être réévaluée régulièrement par la direction afin qu'elle reste pertinente, conforme à la réalité. Il est important, en l'occurrence, de communiquer, d'expliquer et de répéter régulièrement les procédures et notes de corps élaborées (au moyen de campagnes de sensibilisation) ;*
- *les mesures de maturité ainsi que les analyses de risque et de vulnérabilité sont des piliers importants dans la politique de sécurité et contribuent à une sécurité optimale des informations, basée sur les risques. Le budget-temps de la DPO fait aussi partie de cette gestion des risques ;*
- *l'élaboration de procédures formelles de concertation et de communication avec toutes les parties concernées au sein de la ZP de telle sorte que la DPO soit impliquée davantage dans les activités de l'organisation et dispose toujours des informations nécessaires pour l'exécution de la mission qui lui a été confiée.*

4.7.2. Fichiers de journalisation des propres systèmes ICT (« traçabilité »)

85. À partir des réponses et de la documentation transmises, le COC n'a pas pu établir l'existence de fichiers de journalisation pour divers systèmes et applications ICT internes[103] afin de garantir la traçabilité des actions et de pouvoir procéder à un examen rétroactif des incidents. Il n'existe pas de politique formelle et de documentation relatives à la gestion des fichiers de journalisation (quelles sont les informations journalisées, les règles en matière de délais de conservation, les modalités d'accès, etc.). Des contrôles proactifs des fichiers de journalisation ne sont pas effectués, ils ne le sont que sur demande (base *ad hoc*). Il n'existe pas de plate-forme centralisée de gestion des journaux ou d'outil *SIEM*[104]. Le COC renvoie à ce propos à la mesure correctrice dans le numéro 36 dans le cadre de traitements de

[102] Par plan de sécurité des informations, il faut entendre : un plan basé sur une analyse de risque pour mettre en oeuvre les mesures manquantes de protection des informations de telle sorte que les objectifs de sécurité formulés dans la politique de sécurité soient poursuivis au maximum.
[103] Donc pas ceux gérés par la DRI.
[104] *Security Information and Event Management*.

données à caractère personnel, la gestion des fichiers de journalisation devant toujours respecter les dispositions de l'article 56 de la LPD.

Recommandation
Il est recommandé d'effectuer une analyse de risque concernant la gestion des fichiers de journalisation et la surveillance des systèmes ICT internes afin d'obtenir les garanties nécessaires relatives à la traçabilité des activités de traitement des données.

4.7.3. Gestion des accès

86. En ce qui concerne la gestion des accès, le COC souhaite souligner l'importance de l'utilisation de comptes nominatifs. L'utilisation d'un compte générique (par exemple, identifiants de service qui peuvent être partagés entre plusieurs personnes) doit être évitée afin de garantir une traçabilité correcte relative aux activités de traitement des données. Les utilisateurs ayant des droits d'accès étendus comme les gestionnaires de système et d'applications (c'est-à-dire les « utilisateurs privilégiés ») doivent exécuter leurs tâches système quotidiennes à l'aide d'un compte d'utilisateur nominatif. Avec des comptes génériques partagés, la détermination du responsable en cas d'abus risque d'être impossible. Par ailleurs, un compte compromis d'un utilisateur privilégié, en raison de droits d'accès étendus, permet en principe d'effacer les traces des activités, par exemple en adaptant les fichiers journaux système ou en les effaçant complètement.

87. Des mesures organisationnelles ou techniques spécifiques ne sont pas prévues pour le contrôle des utilisateurs privilégiés. Ce type d'utilisateur est composé de comptes aux droits d'accès très vastes au sein d'un système ICT, d'une application, d'un environnement ou domaine (par exemple, gestionnaires de système et d'applications).

Recommandation
Le COC insiste pour :

- *autoriser exclusivement l'utilisation de comptes d'utilisateur nominatifs/individuels dans le cadre de la gestion opérationnelle. L'utilisation d'un compte d'utilisateur générique pour la gestion système doit être fortement limitée et est autorisée uniquement si elle est requise techniquement ;*
- *inventorier tous les comptes privilégiés, y compris les comptes de domaine et comptes locaux pour avoir la certitude que seules les personnes autorisées ont des droits majorés ;*
- *faire en sorte que tous les utilisateurs ayant accès à un compte privilégié utilisent un compte nominatif spécial ou secondaire pour l'exécution d'activités ICT qui nécessitent des droits majorés. Ce compte privilégié peut seulement être utilisé pour ces activités administratives et non pour exécuter des activités opérationnelles quotidiennes, surfer sur Internet, échanger des e-mails ou des activités similaires ;*
- *reprendre toutes les activités relatives à l'utilisation et à la gestion de ces comptes privilégiés dans des fichiers de journalisation et prévoir des mesures protégeant l'intégrité pour ces fichiers de journalisation.*

4.7.4. *Planification de la continuité*

88. La ZP a commencé à formuler un plan de continuité ICT dans lequel plusieurs actifs essentiels (notamment les serveurs et le réseau) ne sont cependant pas encore intégrés. Sur la base des informations reçues, le COC n'a pu parvenir à la conclusion que des tests *DRP*|*BCM*[105] étaient prévus systématiquement/sur une base périodique[106].

Recommandation
Il est recommandé de prévoir un plan de reprise après sinistre ICT (DRP ou Disaster Recovery Plan) et un plan de continuité pour tous les processus critiques et systèmes essentiels d'information de l'organisation et de les tester sur une base périodique. Un DRP pour ICT va bien au-delà de prévoir simplement un back-up. Reste à savoir comment préparer l'organisation à tous les sinistres possibles qui peuvent frapper les systèmes ICT.

[105] *Disaster Recovery Plan* (*DRP*)|*Business Continuity Plan* (*BCP*)
[106] Il faut notamment entendre ci-dessous : les tests périodiques de la politique de *back-up*, la simulation d'incidents et de situations de crise (panne de courant, défaillance d'un composant système, absence du personnel clé, etc.).

5. CONCLUSION – RECOMMANDATIONS – MESURES CORRECTRICES

Conclusion

89. Seul un nombre minime d'aspects des thèmes contrôlés s'avèrent conformes à la législation. En ce qui concerne les aspects prépondérants sur le plan de la protection des données, il apparaît que la ZP a bien l'ambition de pouvoir apporter une réponse à certaines matières sensibles mais elle en a été empêchée en partie par le budget-temps effectif minime, d'une part, et l'absence d'une documentation détaillée concernant les aspects correspondants, d'autre part (ICT et sécurité des informations), nonobstant l'engagement évident des membres du personnel désignés et de la *DPO*.

90. La constatation générale précédente traduit les manquements constatés concrets. Surtout dans le domaine de l'utilisation de la surveillance par caméra et de l'application du cadre légal relatif au droit en matière de protection des données, différentes démarches doivent encore être entreprises. En revanche, la ZP affiche un très bon fonctionnement de la gestion fonctionnelle.

91. Bien que plusieurs directives de corps, relatives à la sécurité des informations, aient été établies, la ZP n'a pas de plan général de sécurité des informations et de continuité, ciblé sur les risques, dans le cadre duquel l'organisation et, en particulier, le service ICT, puisse inscrire ses propres mesures. Une telle approche fondée sur les risques permettrait d'évaluer, de formaliser et de documenter les mesures prises. Le service ICT de la ZP prévoit une série d'initiatives de sécurité ICT mais le contrôle (interne/externe) périodique du bon fonctionnement et de l'exhaustivité de ces initiatives n'est pas assuré d'une manière structurelle et formelle.

L'implication de la DPO dans le suivi, la rectification et la mise en œuvre de la politique de sécurité des informations et de protection des données doit être renforcée. Une approche structurelle et un suivi périodique sont indiqués en l'occurrence.

Par conséquent, une série de recommandations s'imposent et doivent contribuer à une amélioration de l'efficacité et de l'efficience du traitement de données (à caractère personnel) par la ZP.

Les manquements légaux constatés incitent cependant l'Organe de Contrôle à prendre des mesures correctrices, la ZP devant régulariser la situation dans un délai déterminé.

PAR CES MOTIFS,

L'Organe de Contrôle de l'Information policière,

Formule la demande et les recommandations suivantes ;

Prend les mesures correctrices suivantes,

<u>Demande</u>

que le chef de corps, en attendant l'arrêté d'exécution relatif au registre local des caméras, constitue un registre local de l'utilisation de caméras ou l'insère dans un volet séparé du registre des traitements en indiquant clairement les types de caméras, les finalités et le support d'enregistrement des images.

<u>Recommandations</u>

1) <u>Recommandation</u>
En vue d'une application effective et efficace des traitements *ANPR*, il est important que la ZP élabore une politique claire d'intervention pour les *hits* sur les listes nationales et une politique claire d'action et d'intervention sur les listes locales.

2) <u>Recommandation</u>

L'Organe de Contrôle insiste pour l'élaboration d'une *policy/*politique qui permette de mettre en place un mécanisme efficace assurant une surveillance continue des profils et une gestion en temps réel des accès en fonction des effectifs réels.

3) Recommandation
Le COC insiste pour que la ZP définisse dans une note de corps une politique pour la constitution de banques de données particulières reprenant les paramètres sur la base desquels s'opère le contrôle de la conformité de la constitution d'une banque de données particulière pour cette activité de traitement déterminée aux conditions légales de l'article 44/11/3 de la LFP.

4) Recommandation
Il importe que le chef de corps opère, dans l'ordre du corps, une distinction claire entre les divers aspects visés sur le plan de l'accès et de l'utilisation d'Internet et des réseaux sociaux pour des objectifs personnels et professionnels et de l'utilisation ou non d'appareils personnels[107]. C'est ainsi que l'accès à Internet (recherches, sites autorisés et interdits) pendant les heures de service doit être distingué de l'utilisation des réseaux sociaux pendant les heures de service à des fins personnelles, d'une part, et dans la mesure où des informations policières pourraient être partagées, d'autre part. Dans un volet séparé ou un document distinct, l'utilisation d'appareils mobiles privés à des fins opérationnelles et l'utilisation d'appareils mobiles professionnels à des fins personnelles doivent être décrites (séparément). En l'occurrence, il importe que le document décrive clairement ce qui est autorisé et interdit, dans quelles circonstances et à quelles conditions un contrôle peut être effectué, quelles sont les conséquences de la constatation d'infractions au document et les droits de la personne concernée dans ce cadre. Il est donc primordial d'opérer une distinction claire entre les divers aspects et finalités en élaborant une procédure qui définit concrètement les principes de base de la transparence et les droits de la personne concernée. C'est également le cas en ce qui concerne l'utilisation d'images de caméras opérationnelles pour le contrôle du respect des conditions de travail.

5) Recommandation
Le COC insiste sur une rectification du budget-temps pour la *DPO* et sur la limitation du nombre de zones de police pour lesquelles elle exerce un rôle coordinateur en tant que *DPO*, à moins que les *DPO* assistants puissent effectivement exercer leur mission de manière autonome. Le COC estime que, dans les circonstances actuelles, la *DPO* ne peut pas disposer de moyens suffisants (temps) pour exécuter correctement les tâches de *DPO* pour le grand nombre de zones de police dans lesquelles elle a été désignée.

6) Recommandation

Il est recommandé de reprendre les points d'action suivants dans le plan de sécurité des informations :

- la poursuite de l'élaboration et l'affinement de la politique en matière de sécurité des informations et de protection des données par le biais de directives du corps et de procédures. Cette politique doit être réévaluée régulièrement par la direction afin qu'elle reste pertinente, conforme à la réalité. Il est important, en l'occurrence, de communiquer, d'expliquer et de répéter régulièrement les procédures et notes de corps élaborées (au moyen de campagnes de sensibilisation) ;
- les mesures de maturité ainsi que les analyses de risques et de vulnérabilité sont des piliers importants dans la politique de sécurité et contribuent à une sécurité optimale des informations, basée sur les risques. Le budget-temps de la *DPO* fait aussi partie de cette gestion des risques ;
- l'élaboration de procédures formelles de concertation et de communication avec toutes les parties concernées **au sein de la ZP** de telle sorte que la *DPO* soit impliquée davantage dans les activités de l'organisation et dispose toujours des informations nécessaires pour l'exécution de la mission qui lui a été confiée.

7) Recommandation
Il est recommandé d'effectuer une analyse de risque concernant la gestion des fichiers de journalisation et la surveillance des systèmes ICT internes afin d'obtenir les garanties nécessaires relatives à la traçabilité des activités de traitement des données.

[107] L'Organe de Contrôle attire l'attention en l'occurrence sur les réglementations légales qui protègent la confidentialité de la communication privée, comme l'article 314bis du Code pénal et la loi du 13 juin 2005 « *relative aux communications électroniques* » qui protège la confidentialité des télécommunications (article 5 de cette loi).

8) Recommandation
Le COC insiste pour :

- autoriser exclusivement l'utilisation de comptes d'utilisateur nominatifs/individuels dans le cadre de la gestion opérationnelle. L'utilisation d'un compte d'utilisateur générique pour la gestion système doit être fortement limitée et est autorisée uniquement si elle est requise techniquement ;
- inventorier tous les comptes privilégiés, y compris les comptes de domaine et comptes locaux pour avoir la certitude que seules les personnes autorisées ont des droits majorés ;
- faire en sorte que tous les utilisateurs ayant accès à un compte privilégié utilisent un compte nominatif spécial ou secondaire pour l'exécution d'activités ICT qui nécessitent des droits majorés. Ce compte privilégié peut seulement être utilisé pour ces activités administratives et non pour exécuter des activités opérationnelles quotidiennes, surfer sur Internet, échanger des e-mails ou des activités similaires ;
- reprendre toutes les activités relatives à l'utilisation et à la gestion de ces comptes privilégiés dans des fichiers de journalisation et prévoir des mesures protégeant l'intégrité pour ces fichiers de journalisation.

9) Recommandation
La ZP est encouragée à renforcer la surveillance et les contrôles afin de pouvoir disposer d'une vision correcte et actuelle du fonctionnement et de l'efficacité de la protection intégrale des informations. Cela implique notamment de :

- veiller au respect des obligations légales, réglementaires et contractuelles et de ses propres lignes politiques relatives à la sécurité des informations et, en particulier, au traitement de données à caractère personnel ;
- contrôler régulièrement la conformité des systèmes d'information avec les normes pour l'exécution de la protection et la mesure de la conformité technique. L'exécution de *vulnerability scans*, de *penetration testing* et de *security audit/review* peut notamment être utile à cet effet ;
- une analyse périodique réalisée par un tiers indépendant est une plus-value absolue.

10) Recommandation
Il est recommandé de prévoir un plan de reprise après sinistre ICT (*DRP* ou *Disaster Recovery Plan*) et un plan de continuité pour tous les processus critiques et systèmes essentiels d'information de l'organisation et de les tester sur une base périodique. Un *DRP* pour ICT va bien au-delà de prévoir simplement un *back-up*. Reste à savoir comment préparer l'organisation à tous les sinistres possibles qui peuvent frapper les systèmes ICT.

Mesures correctrices

Étant donné les articles 221 § 1 et 247, 4°, 5° et 6° de la LPD ;

Charge la ZP :

a) de conformer l'accès aux images des caméras avec l'article 25/7 § 1, troisième alinéa de la LFP afin que le motif des consultations soit enregistré. La preuve de cette mise en œuvre conforme à la loi sera soumise dans les neuf mois suivant la date de la notification de cette mesure correctrice à l'Organe de Contrôle ;

b) de tenir à jour les fichiers de journalisation de l'accès aux images des caméras conformément à l'article 56 de la LPD. La preuve de cette mise en œuvre conforme à la loi sera soumise dans les neuf mois suivant la date de la notification de cette mesure correctrice à l'Organe de Contrôle ;

c) d'expliquer les critères d'insertion sur les listes *ANPR* locales et de les transmettre à l'Organe de Contrôle dans les trois mois suivant la date de la notification de cette mesure correctrice à l'Organe de Contrôle ;

d) de consulter régulièrement les journalisations de la BNG et d'effectuer des contrôles proactifs par coups de sonde (2 x/an) dans le but de surveiller l'introduction obligatoire d'un motif de consultation et les consultations irrégulières éventuelles et ce une première fois dans les six mois qui suivent la notification de cette mesure correctrice et d'en mettre leurs résultats à la disposition du COC ;

e) d'établir un plan de sécurité des informations. Le plan de sécurité des informations sera mis à la disposition de l'Organe de Contrôle dans les neuf mois suivant la date de la notification du présent rapport ;

Dit pour droit que la date de début des mesures correctrices et la date de leur notification visée aux lettres a) à e) inclus doit se comprendre comme la date de la transmission du rapport définitif actuel de l'Organe de Contrôle par e-mail contre accusé de réception augmentée de deux jours.

L'Organe de Contrôle indique la possibilité pour les parties d'interjeter appel dans les trente jours suivant la décision de l'Organe de Contrôle auprès de la cour d'appel du domicile ou du siège du demandeur (article 248 § 1er, premier alinéa et § 2 de la LPD).

Ainsi décidé par l'Organe de Contrôle de l'Information policière le 17 février 2021.

Pour l'Organe de Contrôle

Philippe Arnoud
Président

Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière