CONTRÔLE RESTREINT

RAPPORT DU CONTRÔLE RESTREINT DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SA COMPÉTENCE DE SURVEILLANCE ET DE CONTRÔLE CONCERNANT LE PARTAGE D'IMAGES DE CAMERAS ENTRE LE CIC DE FLANDRE ORIENTALE ET LA ZP NINOVE PAR L'ENTREMISE DU REAL TIME INTELLIGENCE CENTER/OSINT-ADMINISTRATIVE

Rapport

Référence : CON22003

0 Table de matière

1 INTRODUCTION

1.1 Résumé

Résumé

Dans plusieurs rapports parus récemment, l'Organe de contrôle de l'information policière (COC) a présenté sa vision d'un réseau de caméras intégré au sein de la police intégrée. Dans les circonstances prévues par la loi, les zones de police et les entités fédérales peuvent et doivent s'échanger des images de caméras. Un cas concret de collaboration entre une entité fédérale et une entité locale a été analysé plus en détail afin de déterminer quels éléments de la vision exposée par le COC pouvaient déjà être mis en pratique et à quels obstacles cette mise en œuvre se heurtait.

Dans le présent rapport, l'Organe de contrôle choisit surtout de formuler des suggestions d'optimalisation du fonctionnement de la GPI[1] *sensu lato*, et n'opte donc pas pour une approche correctrice (restreinte) à l'égard des entités de police interrogées et visitées.

Mots-clés

Réseau de caméras – intégré – *Video Management System* (*VMS*) – modèle vidéo fonctionnel – AIPD – *DPIA* – responsable du traitement – sous-traitant – fournisseur – *MS Teams*

[1] Geïntegreerde Politie – Police Intégrée.

1.2 Prise en connaissance des faits

1. Le COC apprend dans un article publié dans le quotidien *Het Nieuwsblad* le 16-05-2022 (pièce 1) que le *Real Time Intelligence Center* (*RTIC*) du SICAD[2] de la DCA[3] de Flandre orientale est en mesure de visionner directement des images de caméras installées sur le territoire de la ZP Ninove, et ce dans le cadre d'un 'projet pilote'. Le COC n'est pas à même de déduire de l'article qui est le responsable du traitement des caméras de la ZP Ninove, ni de quelle réglementation celles-ci relèvent (la LFP[4] ou la loi caméras), ni donc en vertu de quelles dispositions légales le *RTIC* traite ces images.

Le COC apprend par ailleurs que de nombreux aspects juridiques et techniques ont dû être réglés pour permettre la mise en place du projet.

2. Article paru dans le quotidien *Het Nieuwsblad* le 16-05-2022 :

Lancement d'un projet pilote permettant la transmission directe d'informations importantes à la police fédérale. La centrale d'urgence a accès en temps réel aux images des caméras de la ville : « Plus rapide et plus efficace »

La ville de Ninove et la police fédérale de Flandre orientale ont lancé en début d'année un projet pilote permettant à la centrale d'urgence de visionner directement les images de dizaines de caméras installées dans la ville. De cette manière, les équipes peuvent être plus rapidement et plus efficacement déployées et commandées sur le terrain lors d'incidents.

Ninove a initié dès 2015 un déploiement échelonné de caméras, une manière pour la ville d'investir dans la sécurité de ses habitants. « Nous avons aussi notre propre régie qui nous permet de visionner régulièrement nous-mêmes les images des caméras, de manière à pouvoir au besoin intervenir sur le terrain. », explique Tania De Jonge, bourgmestre de Ninove (Open VLD). Le Centre d'Information et de Communication (CIC) de la police fédérale a également créé en 2019 une équipe Real Time Intelligence (RTI), dont le rôle est de veiller à soutenir au maximum les équipes sur le terrain en leur fournissant le plus possible d'informations additionnelles pendant le dispatching.
Source d'informations
Le réseau et le système de caméras de Ninove ayant plusieurs points communs avec celui utilisé par le CIC, les deux parties se sont dans le courant de 2020 mises à envisager le lancement d'un projet pilote qui permettrait aux images des caméras de Ninove d'être directement visionnées au CIC. Les images des caméras de surveillance constituent une source cruciale d'informations. Lorsqu'un incident se produit dans une rue et que quelqu'un prend la fuite, les images des caméras peuvent être d'une aide précieuse. Après une période d'essai, le projet pilote a d'emblée prouvé sa plus-value dans le cadre de l'approche des bandes occasionnant des nuisances et des interventions lors de bagarres. « La police de Ninove est très satisfaite de la collaboration. », explique Leen Vanhandenhove, porte-parole de la zone de police. « Cette méthode de travail axée sur l'information profite à la sécurité de nos collaborateurs et des citoyens. ».
Pas d'enregistrement
Concrètement, l'équipe de la centrale d'urgence est en mesure de consulter et d'exploiter les images. Les images des caméras restent disponibles pour consultation pendant trois heures, mais ne sont jamais enregistrées. « Lorsque nous recevons un appel d'urgence concernant un fait survenu à Ninove, nous pouvons immédiatement consulter les images des caméras concernées. De cette manière, les équipes de la police locale peuvent être plus rapidement dépêchées sur les lieux. », explique Jeroen Duville, chef de service de l'équipe Real Time Intelligence de la police fédérale.
« Le projet pilote va à présent être testé pendant une certaine période. Ensuite, on examinera s'il convient de procéder à des adaptations et si d'autres zones de police peuvent adhérer au projet, car la criminalité ne s'arrête évidemment pas aux frontières de la commune. », ajoute Tania De Jonge, bourgmestre. « Des contacts ont d'ores et déjà été établis

[2] Le service d'information et de communication de l'arrondissement, composé du pilier CIC et du pilier CIA. Le CIC est le Centre d'Information et de Communication, responsable du suivi en temps réel à travers la prise en charge des appels et le dispatching des équipes sur le terrain. Le CIA est le deuxième pilier du fonctionnement du SICAD, en charge du traitement de deuxième ligne de l'information.
[3] Direction de coordination et d'appui au sens de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (LPI) et de la loi du 5 août 1992 sur la fonction de police (LFP).
[4] Loi du 5 août 1992 sur la fonction de police.

avec d'autres zones de police de Flandre orientale en vue d'élargir le projet. De nombreux aspects juridiques et techniques ont dû être réglés pour permettre la mise en place du projet, mais nous sommes particulièrement fiers de cette réalisation et nous sommes impatients de pouvoir en élargir la portée au sein de la province. », conclut Jeroen Duville."

2 POUR RAPPEL – LA VISION DU COC

3. La vision exposée par le COC[5] au sujet des traitements de caméras intégrés au sein de la GPI est la suivante. Le PCN[6], en sa qualité de composant national de la GPI, les 10 cellules de transmission des CIC provinciaux[7] en leur qualité de composants décentralisés de la GPI, de même que l'Appui aérien (DAFA) de la police fédérale et nombre de dispatchings des zones de police locale disposent d'un « *Video Management System » (VMS*), qui permet le suivi en temps réel d'images ainsi que leur enregistrement et leur traitement.

Les *VMS* fédéraux, à savoir ceux du PCN, des cellules de transmission des CIC et de l'Appui aérien, sont déjà reliés entre eux afin de pouvoir recevoir les images des hélicoptères et/ou des drones de DGA/DAFA, qui sont captées au moyen de 8 antennes et transmises au *VMS* de DGA/DAFA. Ce système et les *VMS* participants constituent donc *de facto* un *backbone* de la solution qui pourrait par la suite être déployée à l'échelle nationale. Ce *backbone*, qui est relié aux réseaux de fibre optique nationaux et régionaux qui ont été connectés au centre de données de la GPI grâce au déploiement du réseau national de caméras ANPR, pourrait donc être utilisé pour recevoir et rendre accessibles les images tant des caméras de la police (relevant de la LFP) que des caméras de tierces parties (relevant de la loi caméras), et même éventuellement à terme des appels vidéo de citoyens.

Un Video Management System, également appelé *Video Management Software* ou *Video Management Server*, est un composant d'un système de surveillance par caméra qui, d'une manière générale :

- rassemble des images de caméras et d'autres sources ;
- enregistre les images ;
- offre une interface permettant à la fois de visualiser les vidéos en direct et d'accéder aux images enregistrées.

Du fait des améliorations intervenues au niveau de la technologie, il y a lieu de faire une distinction entre un *Video Management System (VMS)* et les fonctions intégrées des caméras modernes fonctionnant en réseau. Des nombreuses caméras modernes fonctionnant en réseau offrent des fonctionnalités internes permettant d'enregistrer directement des images vidéo et de les visualiser dans un navigateur Internet sans recourir à un *VMS*. Ces possibilités existent aussi pour les caméras montées sur des drones, et vont de l'enregistrement sur la carte SD au *streaming* des images. Pour une approche **intégrée** de l'utilisation policière de caméras, un *VMS* est donc requis.

4. Un *VMS* permettrait aussi une gestion efficace et intégrée de l'utilisation de caméras. Si les différents *VMS* qui existent au sein de la GPI venaient à s'intégrer en un seul système de surveillance vidéo disposant d'un statut juridique consolidé et d'un modèle vidéo fonctionnel propre, la synergie vidéo entre la GPI et ses partenaires externes s'en trouverait considérablement facilitée : des conventions et des protocoles standard, des AIPD types et une seule connexion technique suffiraient alors à mettre en place l'échange d'images de caméras. Les *VMS* formeraient ainsi un portail d'accès pour les images de caméras pouvant être utilisées par la police, ce qui pourrait d'une part induire un risque en l'absence des mesures de mitigation adéquates, mais offrirait d'autre part des avantages considérables en termes de qualité de la gestion des données et de réduction du risque d'abus des données ; une politique de sécurité uniforme pourrait être appliquée et offrir des garanties fiables en termes de traçabilité et de confidentialité des données, ce qui ne ferait que profiter à l'utilisation opérationnelle de caméras par la police.

[5] CON20004 et DIO20009 (publiés) ; DIO23004 (uniquement disponible en interne au sein de la GPI).
[6] **P**oint de **c**ontact **n**ational.
[7] CIC est l'acronyme de Centre d'Information et de Communication, à savoir le premier pilier du fonctionnement provincial du SICAD, qui est responsable du suivi en temps réel à travers la prise en charge des appels et le dispatching des équipes sur le terrain. Le CIA est le deuxième pilier du fonctionnement du SICAD, en charge du traitement de deuxième ligne de l'information.

3 OBJECTIF DU CONTRÔLE ET MÉTHODOLOGIE

5. À la lumière de la vision exposée par le COC au sujet d'un réseau de caméras intégré au sein de la police intégrée, le DirCoM du COC a dans le sillage de l'article susmentionné initié le 19-05-2022 une enquête de contrôle en chargeant le Service d'Enquête du COC (DOSE) d'interroger le DirCo[8] de Flandre orientale au sujet (pièce 2) :

1) de tous les documents disponibles concernant :
   - le projet pilote proprement dit de la ZP Ninove ;
   - le déploiement du *RTIC* au sein du SICAD de la Flandre orientale ;
2) des aspects juridiques et techniques devant manifestement encore être réglés dans le cadre du projet pilote.

6. Dans le sillage de la mission confiée au DirCoM du COC et afin de pouvoir procéder à une analyse *prima facie*, les pièces suivantes ont été demandées 23-05-2022 au DirCo de Flandre orientale (pièce 3) :

1) au sujet du projet pilote des caméras de Ninove :
   - le fondement juridique de ces traitements de caméras : loi caméras, LFP, … ;
   - si une AIPD[9] a ou non déjà été établie et, dans l'affirmative, une copie de cette AIPD ;
   - des fiches de projet, présentations, schémas fonctionnels, techniques et de processus décrivant le concept de la structure (*high level*) ;
   - les notes de service et directives internes consacrées spécifiquement à ces traitements de caméras ;
2) au sujet du déploiement du *RTIC* au sein du SICAD :
   - les notes de service et directives internes relatives au fonctionnement du *RTIC* ;
   - des présentations décrivant ce fonctionnement.

7. Dans son accusé de réception du 23-05-2023, le DirCo de Flandre orientale a fait savoir que la ZP Ninove gère une importante quantité de documentation et qu'il rassemblerait et transmettrait par conséquent toute la documentation demandée en concertation avec cette zone de police (pièce 4).

8. Dans le sillage de la demande du COC, il est apparu que des actualisations étaient requises auprès des deux entités de police (pièce 5). Le 10-08-2022, le DirCo de Flandre orientale a transmis un certain nombre de documents par e-mail (pièce 6) :

- l'AIPD de la ZP Ninove et de la DCA, établie par le DPO de la ZP Ninove et le DPO de la DCA de Flandre orientale et actualisée le 08-08-2022 (pièce 7) ;
- l'AIPD de la ZP Ninove et de la DCA, établie le 22-02-2021 (ancienne version ayant entretemps été actualisée) (pièce 8) ;
- le protocole de protection de la vie privée du 07-07-2022 de la ZP Ninove et de la DCA de Flandre orientale, signé par le DirCo ; la signature par le chef de corps est prévue dans les meilleurs délais (pièce 9) ;
- les règles de fonctionnement de la ZP Ninove (telles que publiées sur le *Sharepoint*) (pièce 10) ;
- les règles de fonctionnement de l'équipe RTI du CIC de Flandre orientale (telles que publiées sur le *Sharepoint*) (pièce 11).

Le DirCo de Flandre orientale a en outre invité le COC à une visite sur place afin de pouvoir se rendre compte du fonctionnement en temps réel et de recevoir toutes les explications à ce sujet. Le COC a répondu qu'il procéderait aux analyses nécessaires et tiendrait le DirCo informé (pièce 12).

9. Il ressort de l'analyse des documents qu'en marge des aspects juridiques, il convient également de poser de nombreuses questions techniques.

[8] Le directeur coordonnateur administratif d'arrondissement de la police fédérale au sens de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (LPI) et de la loi du 5 août 1992 sur la fonction de police (LFP).
[9] Analyse d'impact relative à la protection des données, en anglais *DPIA* pour *Data Protection Impact Assessment*.

10. La première analyse des documents transmis permet toutefois d'établir que l'application *MS Teams* du progiciel O365 de Microsoft, en usage au sein de la GPI, joue un rôle dans l'échange des images entre le *RTIC* et la ZP Ninove. Le COC pose dès lors en date du 18-08-2022 un certain nombre de questions à d'autres entités de police au sujet du rôle de *MS Teams* dans les traitements de caméras de la GPI :

1) à la DGA/DAS[10] (pièce 13) ;
2) à la DGA/DAFA[11] (pièce 14) ;
3) à la DGR/DRI[12] (pièce 15).

11. Le 18-08-2022, la DGA/DAS répond qu'elle n'utilise pas l'application *MS Teams*, mais qu'elle dispose en revanche d'une communication alternative recourant à un serveur propre (pièce 16).

12. Le 19-08-2022, le COC prend connaissance d'un concept de « Plateforme vidéo GPI » réservant également un rôle à *MS Teams* (pièce 17). Cela cadre dans la vision exposée le 08-09-2022 par le DPO de la DGA/DAS, dans laquelle ce dernier indiquait être également intéressé par l'utilisation de *MS Teams* dès lors que cette application pourrait offrir une plus-value (pièce 21).

13. Le 22-08-2022, la DRI de la DGR (pièce 18) répond en joignant à sa réponse une note DRI 2019/5304 établie au niveau du corps en date du 11-06-2019, intitulée *Guide d'utilisation des solutions 'police cloud' (Microsoft 365) au sein de la police intégrée* (pièce 19).

14. Le 12-09-2022, DGA/DAFA répond (pièce 20) en indiquant avoir déjà utilisé *MS Teams* à quelques reprises. Le 23-09-2022, DGA/DAFA explique concrètement comment cela se passe (pièce 22).

15. En poursuivant ses analyses en interne, le COC établit un questionnaire en préparation de sa visite sur place au SICAD/CIC/*RTIC* de Flandre orientale et à la ZP Ninove. Le 23-11-2023, ce questionnaire est transmis aux deux responsables du traitement (pièce 23).

16. Le 27-11-2023, le DirCo de Flandre orientale fait savoir que les éléments de réponse seront établis conjointement (pièce 24). Il avance également février 2024 comme date pour une visite sur place aux deux entités de police.

17. Le 05-02-2024, le COC reçoit les éléments en réponse aux questions posées le 23-11-2023 (pièce 25).

18. Les visites sur place ont lieu à Gand le 30-04-2024 à 10h00 (pièces 30 et 33) et à Ninove le 30-04-2024 à 13h00 (pièces 29 et 33).

19.1. Le 18-08-2025, le projet de rapport est transmis pour prélecture avec droit de réponse au chef de corps de la ZP Ninove et au DirCo de Flandre orientale (pièce 34).

19.2. Le 08-09-2025, le DirCo de Flandre orientale répond au COC qu'il n'a rien à ajouter au projet de rapport ni aucune question à poser à ce sujet et ajoute avoir l'intention, après la publication du rapport définitif, d'examiner avec le chef de corps de la ZP Ninove et le DPO de la ZP Ninove quels points d'action peuvent être résolus à leur niveau. Il ajoute cependant que la collaboration dans le cadre des images de caméras est pour ainsi dire au point mort étant donné que le CIC de Flandre orientale ne dispose en ce moment d'aucune capacité de RTI (pièce 35).

19.3. Le 12-09-2025, le chef de corps de la ZP Ninove répond au COC qu'il n'a rien à ajouter à ce rapport ni aucune question à poser à ce sujet. En collaboration avec le DPO de la zone de police Dender-Schelde et la DCA de Flandre orientale, la ZP Ninove examinera les points d'action soulevés afin de déterminer à quelles adaptations il peut être procédé à leur niveau.

---

[10] La Direction de la sécurité publique (DAS) est l'unité d'appui centralisée qui fait partie de la DGA et qui fournit en cette qualité à toutes les entités de la GPI différentes formes de renfort en matière de gestion négociée de l'espace public, en particulier les équipes et moyens spécialisés dans la prévention et la résolution de situations violentes ou dangereuses.

[11] L'Appui aérien (DAFA) est un service de police spécialisé qui appuie la police fédérale et la police locale depuis les airs, et ce afin d'assurer une fonction de police de meilleure qualité et plus efficace. Les moyens aériens sont engagés d'une part pour récolter des informations (policières) et d'autre part comme moyen d'intervention (ex. le *dropping* d'eau).

[12] La Direction de l'information policière et des moyens ICT (DRI de la DGR) est responsable du concept de l'information policière, de la préparation du traitement de l'information et des systèmes de communication, des normes techniques, des processus des services d'information et de communication d'arrondissement, de la gestion de la BNG, de la documentation opérationnelle, etc.

Additionnellement, le chef de corps de la ZP Ninove indique que le projet RTI est entretemps devenu un projet dormant du fait que la DCA de Flandre orientale ne dispose d'aucune capacité à affecter à la RTI. Le chef de corps de la ZP Ninove ajoute que la ZP Ninove assurera à partir d'octobre 2025 une permanence 24 heures sur 24 et 7 jours sur 7 à l'hôtel de police, de sorte qu'elle aura moins besoin du soutien de la DCA pour la vidéosurveillance (pièce 36).

4 CONCLUSIONS DE L'ENQUÊTE

4.1 Introduction

20. Les documents transmis renvoient parfois à de la réglementation non applicable, par exemple au RGPD, ou à des traitements de caméras ne relevant pas du périmètre de l'enquête de contrôle, comme les caméras ANPR ou l'utilisation non visible de caméras par la police. Un chapitre consacré aux normes applicables révèle que ces normes n'existent pas. Les références récurrentes aux caméras de la ville laissent à penser que la police n'est pas l'utilisateur exclusif des caméras. Certains documents, comme l'AIPD conjointe (pièce 7) et le protocole de protection de la vie privée (pièce 9) datent d'**après** les questions posées par le COC ou ont été actualisés dans leur sillage, respectivement le 08-08-2022 et le 07-07-2022. Certains sujets sont plutôt abordés de manière très générale et ne sont pas approfondis. Une recherche sur la présence ou l'absence dans le texte de la MFA[13] – pourtant obligatoire[14] – ne donne par exemple aucun résultat. Aucun des documents transmis ne semble tenir compte des directives ministérielles contraignantes relatives à la sécurité de l'information[15], aux accès[16] ou aux interconnexions[17] prévues à l'article 44/4 de la LFP.

Vu les nombreuses imprécisions, le COC regroupe des questions additionnelles à partir de ses 59 questions et remarques initiales et les transmet à la ZP Ninove et à la DCA de Flandre orientale (pièce 23) afin que ces dernières y répondent soit conjointement, soit pour chaque entité prise séparément, ou afin qu'elles montrent des actions ou des lieux lors des visites sur place planifiées (pièces 29 et 30).

21. Les questions et remarques regroupées par thème sont exposées ci-après et complétées des éléments de réponse fournis par la ZP Ninove et la DCA de Flandre orientale (pièce 25) et par d'autres entités interrogées (pièces 16, 18, 19, 20, 21), de la documentation concernant le modèle vidéo fonctionnel de la GPI (pièce 17) ainsi que des constatations effectuées lors des visites sur place (pièces 29 et 30).

4.2 Relation entre les différents acteurs

4.2.1 La ZP Ninove et la DCA de Flandre orientale

22. Après lecture et analyse des AIPD (pièces 7 et 8), le COC ne parvient pas à établir clairement quelles sont les relations entre la ZP Ninove et la DCA de Flandre orientale, ni à partir de quel angle d'incidence le document a été rédigé. Le COC se demande s'il s'agit d'un concept de 'responsables conjoints du traitement' comme le prévoit l'article 52 de la LPD, ou s'il s'agit d'une relation entre responsable du traitement et sous-traitant conformément à l'article 53 de la LPD. La relation choisie par les deux acteurs influence en effet les protocoles qui en découlent pour les conventions relatives aux obligations, entre autres en ce qui concerne l'exercice du droit d'accès, les fondements juridiques sur lesquels le traitement repose, etc. … (pièce 23). La réponse conjointe des deux entités de police est formulée comme suit (pièce 25) (citation littérale, traduction libre) :

[13] De l'anglais « Multi-Factor Authentication », signifiant authentification reposant sur plusieurs facteurs. Une telle authentification multifacteur repose sur au moins deux des trois éléments suivants : un élément « connaissance » (quelque chose que seul l'utilisateur sait), un élément « possession » (quelque chose que seul le signataire possède) et un élément « qualité » (quelque chose que l'utilisateur est).
[14] Directive commune contraignante des ministres de la Justice et de l'Intérieur du 13 juillet 2021 relative aux règles d'accès des membres des services de police à la banque de données nationale générale, aux banques de données de base, particulières et techniques.
[15] Article 44/4 §2 de la LFP.
[16] Article 44/4 §3 de la LFP.
[17] Article 44/4 §4 de la LFP.

« L'AIPD au sujet de l'utilisation des images de caméras par la ZP Ninove (DCA de Flandre orientale) a été établie par (…) sans que cette AIPD n'ait été communiquée au DPO de la zone de police Dender-Schelde, et donc sans l'accord du DPO de la zone de police Dender-Schelde.

L'AIPD qui a été établie le 8 août 2022 entre la zone de police de Ninove et la DCA de Flandre orientale – SICAD est destinée à préciser l'attribution des rôles dans le cadre de cette AIPD.

Le chef de corps de la zone de police Ninove est le responsable du traitement des traitements de caméras effectués au sein de la zone de police Ninove.

Le DirCo de Flandre orientale est quant à lui le responsable du traitement des missions de police administrative et judiciaire lorsqu'il dirige des équipes de la DCA de Flandre orientale. ».

Les entités de police estiment en outre pouvoir déduire de la correspondance échangée avec le COC que ce dernier considère le DirCo de Flandre orientale comme l'unique responsable du traitement. Le DPO de la zone de police Dender-Schelde, en particulier, qui est le DPO de la ZP Ninove, semble partir à tort du principe que des discussions distinctes auraient eu lieu entre le DirCo de Flandre orientale et le COC, dès lors qu'il affirme :

« Le DPO de la zone de police Dender-Schelde n'a jamais été informé de la teneur de cette ou de ces discussions, ni des adaptations requises. » (citation littérale, traduction libre).

Or, toute la communication du COC a été adressée en toute transparence aux deux entités de police.

4.2.2 La DGR/DRI et *Microsoft* en tant que sous-traitans

23. Initialement, la ZP Ninove et la DCA de Flandre orientale citent *Microsoft* et la DRI en tant que sous-traitants (pièces 7 et 8). Interrogées à ce propos (pièce 23), les deux entités de police formulent la réponse suivante (pièce 25) (citation littérale, traduction libre) :

« Ce traitement – vidéosurveillance exercée par la police sur un lieu non fermé et RTI exercée par la DCA de Flandre orientale – recourt à l'application de la politique d'accès de la GPI, sous la gestion générale de la DRI, à l'environnement Office 365, et spécifiquement à Microsoft Teams, pour la transmission de captures d'écran d'images entre la DCA de Flandre orientale et les collaborateurs opérationnels de la ZP Ninove avec des droits d'accès au canal spécifique en Microsoft Teams.

La DRI est le responsable du traitement en ce qui concerne le progiciel Microsoft 365 et est en cette qualité une partie concernée étant donné que les images de caméras sont partagées en Teams. Le choix du terme 'sous-traitant' dans la version 1.0 de l'AIPD n'était pas un choix réfléchi étant donné que les parties concernées n'effectuent pas de traitements spécifiques. ».

24. La note DRI 2019/5304 (pièce 19) stipule cependant ce qui suit à ce sujet (citation littérale, traduction libre) :

« Chaque membre de la GPI qui utilise les solutions mises à sa disposition en assume la responsabilité. Il est donc tenu de respecter le cadre légal et professionnel en fonction de son unité et de son rôle.

Chaque propriétaire (« owner ») d'un groupe (par ex. le propriétaire d'une équipe en Yammer, en Teams, sur un site du SharePoint, …) qui existe dans le système est responsable de toutes les informations qui sont gérées au sein du groupe en question ainsi que de la gestion proprement dite des membres du groupe. Il doit veiller à ce que les différentes règles en matière de gestion de l'information soient respectées (secret de l'enquête, secret professionnel, protection des données à caractère personnel, etc.).

Les chefs de service sont investis d'une responsabilité de gestion fonctionnelle, identique à la responsabilité qu'ils endossent pour tous les systèmes utilisés par leurs collaborateurs. ».

25. L'AIPD conjointe (pièce 7) affirme également qu'il n'est pas recouru à des *cloud providers* externes. Or, le progiciel Microsoft O365 GPI est décrit comme étant une solution dans le cloud, avec spécifiquement dans ce dossier un rôle particulier réservé à l'application *MS Teams*.

4.2.3 Tein, Genetec et Edesix en tant que sous-traitans

26. Initialement, la ZP Ninove et la DCA de Flandre orientale faisaient mention de Tein, Edesix (ZP Ninove) et Genetec (DCA de Flandre orientale) (pièces 7 et 8), soit dans le texte, soit dans des schémas. Interrogées à ce sujet (pièce 23), les deux entités de police apportent la précision suivante (pièce 25) (citation littérale, traduction libre) :

« La maintenance anti-intrusion est assurée par le sous-traitant. Tein fournit les logiciels et le matériel ainsi que le support au sous-traitant. Genetec Inc. fournit les logiciels au sous-traitant du sous-traitant. Le Genetec Security Center s'occupe des logiciels pour les caméras. Les logiciels pour les bodycams (Edesix) sortent du cadre de la RTI. ».

27. Aucun des documents fournis n'indique de la part des entités privées Tein, Edesix ou Genetec un traitement de données à caractère personnel actif qui serait ordonné par les responsables du traitement. La pièce 10 semble indiquer que Tein joue un rôle dans la gestion des incidents :

« S'il s'agit d'un nouveau manquement, la ZP Ninove contactera Tein dans les meilleurs délais. ».

Les visites sur place n'ont pas non plus permis de déduire qu'une ou plusieurs des entités privées citées traiterait activement des données à caractère personnel pour l'une des entités de la GPI en leur qualité de responsables du traitement (fonctionnels). Il ressort par contre des visites sur place que Tein joue un rôle dans la création d'utilisateurs des *VMS* au sein de la ZP Ninove (pièce 29). Les utilisateurs de la DCA de Flandre orientale sont en revanche créés par la DRI de la DGR (pièce 30). Tein gère également le pare-feu (pièce 29).

28. Il ressort en outre de la réponse conjointe des deux entités de police (pièce 25) qu'une convention de traitement des données a été conclue entre Tein et la ZP Ninove, de même qu'entre Genetec et la DGR/DRI.

4.3 Périmètre du projet

29. Vu le caractère intégré et intégral de la vision exposée par le COC, le COC interroge également les deux entités de police au sujet du périmètre du projet en ce qui concerne les images filmées par les hélicoptères et les drones, mais aussi en ce qui concerne les images filmées par une caméra individuelle, les images traitées dans le cadre de l'article 112*ter* du Code d'instruction criminelle (enregistrement audiovisuel d'une audition à la requête du procureur du Roi) et les images provenant de caméras de surveillance fixes d'une tierce partie (par exemple la Ville ou Infrabel) installées sur le territoire de la ZP Ninove. Il demande en outre si le contrôle du respect des conditions de travail[18] fait partie du périmètre du projet (pièce 23). Des questions sont également posées au sujet du rôle de *CAD*[19] (voir le titre **Fout! Verwijzingsbron niet gevonden.**) et d'*ISLP*[20] (voir le titre 4.6).

30. En ce qui concerne les traitements cités, la réponse conjointe des deux entités de police indique que les images des caméras des hélicoptères, des drones ainsi que celles des caméras individuelles et des caméras filmant les auditions ne relèvent pas du périmètre du projet (pièce 25). Les arguments suivants sont évoqués à ce sujet :

- le visionnage en temps réel des images des hélicoptères est assuré par la police fédérale ; par la suite, les images enregistrées pertinentes peuvent être consultées et saisies ;

[18] Voir l'avis d'initiative BD200007 du 17-08-2020 concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail.
[19] *Computer Aided Dispatching* est une dénomination conjointe qui désigne l'ensemble des applications utilisées en vue de la mise en place d'une cellule de transmission assistée par ordinateur. L'environnement *CAD* se compose de plusieurs composantes matérielles et logicielles. Le COC le considère comme une banque de données de base au sens de l'article 44/11/2 de la LFP.
[20] *Integrated System for Local Police*. Banque de données de base au sens de l'article 44/11/2 de la LFP.

- il serait excessif de laisser la ZP Ninove exploiter des images nationales ;
- aucune des entités de police citées ne dispose de drones ;
- les caméras individuelles de la ZP Ninove ne sont pas dotées d'une fonction *livestream* ; si la PJF[21] de Flandre orientale souhaite obtenir des images, celles-ci peuvent être consultées ou partagées sur la base d'une apostille ;
- les images des auditions audiovisuelles[22] sont conservées sur un serveur distinct, puis enregistrées sur des supports de données externes et ensuite effacées du serveur ;
- les caméras en question appartiennent à la Ville de Ninove, mais la ZP Ninove en est l'utilisateur exclusif et le responsable du traitement ;
- techniquement, le partage d'images des hélicoptères, des drones, des caméras individuelles et des caméras filmant les auditions de la ZP Ninove ou d'images du commissariat de la ZP Ninove ne relève pas du périmètre du projet.

De plus, les entités de police indiquent que l'utilisation des images pour le contrôle du respect des conditions de travail ne relève pas du périmètre du projet. Pourtant, l'AIPD conjointe (pièce 7) y fait allusion lorsqu'elle stipule (citation littérale, traduction libre) :

« Si la vidéosurveillance a (aussi) un rapport avec ou un impact sur les conditions de travail et les prestations du personnel des services de police, le RGPD et la LPD s'appliquent (également) (recommandation 06/2011 de l'APD). Les différentes caméras de la zone de police ont été enregistrées dans le registre de traitement des images. ».

« Les différentes finalités (police administrative, police judiciaire ou gestion du personnel) ont également été consignées dans ce registre et portées à la connaissance du CCB. ».

Le périmètre est finalement décrit en ces termes (pièce 25) :

« Le cycle commence au niveau des caméras de surveillance installées sur le territoire de la ville de Ninove. Les différents systèmes de caméras sont gérés au sein du Video Management System global (VMS). La DCA de Flandre orientale – RTI a accès en temps réel aux images par le truchement d'un VPN avec pare-feu et peut ainsi visionner les images remontant à maximum 3 heures. La DCA de Flandre orientale – RTI soutient les équipes d'intervention de la ZP Ninove en partageant des images ou de brefs fragments au moyen du canal Teams prévu à cet effet. Le cycle prend donc fin auprès de la ZP Ninove, qui peut visionner les images dans le canal Teams. ».

4.4 Rôle de *MS Teams*

4.4.1 Généralités

31. Vu la description sommaire qui est faite dans les pièces 7, 8 et 11 du rôle de *MS Teams* dans les processus de travail, le COC interroge les deux entités de police au sujet du rôle de *MS Teams* (pièce 23). La réponse conjointe des deux entités de police est formulée comme suit (pièce 25) (citation littérale, traduction libre) :

« Teams fait partie du progiciel Microsoft 365. ».

Le cycle décrit dans la pièce 25 et cité ci-dessus fournit un peu plus de clarté. Le processus est décrit dans son intégralité de manière exhaustive par les deux entités de police lors de la visite sur place du 30-04-2024.

4.4.2 Traçabilité et journalisation de *MS Teams*

32. En ce qui concerne la traçabilité et la journalisation des traitements effectués dans le canal *MS Teams*, la réponse conjointe des deux entités de police dit ceci (pièce 25) (citation littérale, traduction libre) :

[21] Police Judiciaire Fédérale.
[22] Pour toute clarté, cette utilisation de caméras ne relève pas du régime d'utilisation de caméras visé dans la LFP.

« Toute personne disposant d'un accès au canal Teams peut visionner ces images. À l'heure actuelle, il est impossible de tracer quel membre du personnel a consulté une image de caméra donnée en Teams. La zone de police Ninove vérifiera avec la DRI s'il existe des possibilités de permettre ce traçage. »

4.4.3 Contrôle de la transmission ultérieure des images

33. Vu la possibilité qui existe de télécharger des données à partir de *MS Teams* et en l'absence d'une politique à ce sujet dans les pièces 7, 8 et 11 transmises, le COC demande comment on contrôle si les images sont éventuellement transmises une fois qu'elles quittent l'environnement *MS Teams* (pièce 23). La réponse conjointe des deux entités de police est formulée en ces termes (citation littérale, traduction libre) :

« Il n'est pas procédé à un contrôle périodique, mais des contrôles sont effectués si le service de Contrôle interne informe la zone de police Ninove de la survenance de certains incidents.

Le code de déontologie s'applique. ».

4.4.4 Politique relative aux appareils mobiles sur lesquels l'application MS Teams est installée

34. Vu la possibilité d'utiliser *MS Teams* sur toutes sortes d'appareils mobiles, le DOSE pose un certain nombre de questions au sujet de la pratique *BYOD*[23] à des fins professionnelles, de l'utilisation privée d'appareils de service et de l'utilisation mixte par des tiers – principalement des membres de la famille – soit d'appareils *BYOD*, soit d'appareils professionnels (pièce 23). Dans leur réponse conjointe, les deux entités de police font savoir (pièce 25) (citation littérale, traduction libre) :

« La zone de police Ninove ne travaille pas avec des appareils mobiles personnels, mais seulement avec des tablettes qui restent auprès de la zone ou que les collaborateurs emportent chez eux lorsqu'ils sont de garde, et qui ne peuvent être utilisées qu'à des fins professionnelles. Certains collaborateurs utilisent Teams sur leur appareil personnel de leur propre initiative.

La zone de police Ninove a établi un règlement concernant l'utilisation d'Internet et des appareils mobiles.

La DCA de Flandre orientale dispose d'un règlement pour la gestion des groupes Teams, des ordinateurs de bureau, des ordinateurs portables et des smartphones. Pour ces deux derniers types d'appareils, la situation est réglementée qu'il s'agisse d'appareils privés ou d'appareils achetés par la direction. Ce règlement a été publié sur un site du Sharepoint et est accessible à tous les membres du personnel de la DCA de Flandre orientale. ».

4.4.5 Alternatives à *MS Teams*

35. Interrogées au sujet des technologies autres que *MS Teams* utilisées pour la transmission d'images (pièce 23, dans laquelle il est notamment fait référence à *Astrid Picture Push*[24] et aux points d'accès avec abonnements de données mobiles (téléphoniques)), les entités de police fournissent dans leur réponse conjointe l'explication suivante (pièce 25) (citation littérale, traduction libre) :

« Cette information n'est pas connue pour la ZP Ninove.

La DCA de Flandre orientale ne recourt pas à ces technologies parce qu'elle veut garder le contrôle des informations fournies étant donné qu'il n'y a pas d'autre ventilation. ».

[23] *Bring Your Own Device* : le collaborateur utilise sur une base volontaire ses propres appareils. La sécurisation n'est pas uniforme, dépend de l'utilisateur et est de ce fait souvent moins bien garantie ; l'appareil est également utilisé à des fins privées et la gestion des appareils est (plus) complexe pour l'organisation.

[24] *Picture Push* est une fonction qui est propre au Mobile Data Connectivity Server (MDCS) d'ASTRID et qui permet d'envoyer des photos vers des terminaux mobiles. Pour l'instant, il est seulement possible d'envoyer des photos à des radios TETRA, mais il sera par la suite possible d'en envoyer également à des appareils mobiles (tablettes, ordinateurs portables, smartphones, …) équipés d'une carte SIM Blue Light Mobile (BLM).

36. La DGA/DAS semble disposer d'une solution propre pour la transmission d'images (pièce 16) (citation littérale, traduction libre) :

« Au sein de la DAS, nous n'utilisons pas l'application Teams pour envoyer des images.

La raison en est qu'il s'agit généralement de fichiers trop volumineux (plusieurs giga-octets). Notre unité dispose en effet d'appareils permettant d'obtenir des images en 4K. La qualité des images est meilleure, mais l'inconvénient est que les fichiers sont plus volumineux.

La DAS dispose d'un serveur sur lequel les images sont placées.

Le logiciel crée un lien unique pour chaque fichier à transmettre. Ce lien est lié à un mot de passe. Le lien avec le mot de passe est ensuite transmis au destinataire des images par le biais de la messagerie électronique de la police.

En cliquant sur le lien, le destinataire des images est directement redirigé vers notre serveur, d'où il peut alors télécharger les images.

Nous sommes également en mesure de limiter la possibilité de téléchargement dans le temps ou de limiter le nombre de fois que le fichier peut être téléchargé. S'il s'agit de plusieurs dizaines de giga-octets, nous transférons les images sur un support de données portable ou nous demandons à l'entité de passer chez nous avec un ordinateur portable afin de procéder au transfert. ».

Une réplique du DPO de la DGA/DAS au sujet du même traitement laisse toutefois transparaître un certain intérêt pour l'application *MS Teams*, même si le DPO interrogé a quelques doutes à ce sujet (pièce 21) (citation littérale, traduction libre) :

« Cette application a déjà été testée et pourrait offrir une plus-value dans les situations opérationnelles en temps réel. De plus, nous estimons pouvoir nous fier à la sécurité des applications proposées par la DRI.

Dans l'attente d'une éventuelle prise de position de votre part, il ne nous semble donc pas indiqué de décider d'autoriser ou non l'utilisation de cette application. ».

37. Le modèle vidéo fonctionnel de la GPI (pièce 17) prévoit, en marge d'une interconnexion entre différents *VMS* des différentes entités de police avec un rôle spécifique réservé au SICAD/CIC, également un rôle pour *MS Teams*, même si ce rôle semble se limiter au visionnage en temps réel d'images moyennant un partage d'écran avec un opérateur de l'Appui aérien de la DGA (DAFA). La réaction de la DGA/DAFA semble le confirmer (pièce 20) (citation littérale, traduction libre) :

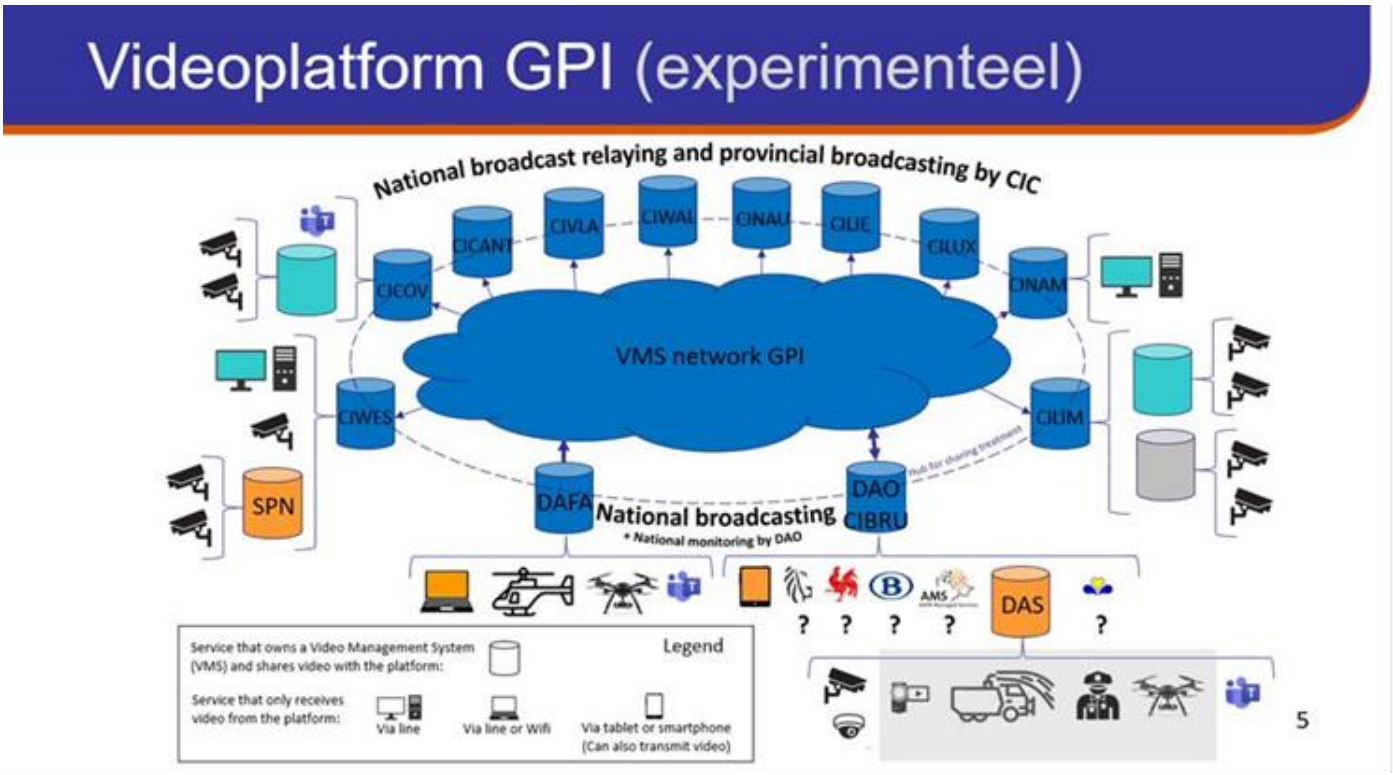
« DAFA a déjà utilisé Teams à quelques reprises pour transmettre des images à des moments où nous rencontrions des problèmes avec la transmission d'images.

Lors des utilisations qui ont été faites de l'application dans le passé, il s'agissait toujours de transmissions à un collègue de la police intégrée et non à des parties externes. ».

Ce point est encore précisé (pièce 22) :

« Les images arrivent sur le serveur de DAFA. Sur l'ordinateur qui gère le serveur, nous démarrons une session Teams avec le « client ». L'écran est partagé de manière à ce que les images soient visibles. ».

Schématiquement, le modèle vidéo conceptuel se présente comme suit (pièce 17) :



Ce modèle est expliqué plus en détail (pièce 17) et peut être résumé en ces termes :

1) Le modèle est destiné tant à la réception qu'à la transmission d'images prises par n'importe quel capteur photographique dont l'utilisation par la police repose sur une base légale ;
2) DAFA et la DAO transmettent les images revêtant un intérêt national au SICAD/CIC. Il s'agit d'images :
   - des caméras des hélicoptères de DAFA (DGA) ;
   - des caméras des drones de n'importe quelle entité de police pour autant qu'elles soient dotées d'un moyen de se connecter au réseau vidéo de la police[25] ;
   - des caméras de la DGA/DAS (par exemple celles montées sur les arroseuses) ;
   - des caméras de services externes à la police, dans le cadre de l'article 25/2 §2 de la LFP.
3) Les CIC transmettent à leur tour aux entités de police intéressées les images :
   - d'intérêt national ;
   - de n'importe quelle entité de police intéressée qui partage ses images avec eux sur une base volontaire ;
   - de tierces parties provinciales.
4) L'offre vidéo est fixée dans les « Standards vidéo de la GPI » ou SVS.

4.5 Rôle de *CAD* dans les processus de travail

38. Interrogées au sujet du rôle de *CAD* dans les processus de travail (pièce 23), les deux entités de police indiquent dans leur réponse conjointe (pièce 25) (citation littérale, traduction libre) :

« Il n'est actuellement pas procédé à l'importation d'images en CAD.

Il est seulement fait mention de l'intervention de RTI dans la fiche d'événement (vérification des caméras, recherches M³). Il existe en CAD une couche désignant les emplacements des caméras. Au moyen du pointeur de l'événement,

[25] Dans le modèle vidéo fonctionnel, il est fait mention du codec vidéo 4G « Soliton ZAO » (qui peut être obtenu en appui).

nous sommes en mesure de déterminer quelles caméras sont présentes à proximité et doivent être surveillées. Le délai de conservation de dix ans est une donnée générale dans le cadre de l'exploitation de la banque de données CAD. ».

En ce qui concerne la « couche » en question de *CAD* désignant les emplacements des caméras, il apparaît lors de la visite sur place (pièce 30) que ceux-ci doivent être créés séparément et qu'il n'y a pas d'échange avec les données des caméras figurant dans le registre de géolocalisation CamELIA prévu à l'article 25/8 de la LFP[26].

4.6 Rôle d' *ISLP* dans les processus de travail

39. Interrogées au sujet du rôle d'*ISLP* dans les processus de travail (pièce 23), les deux entités de police font savoir dans leur réponse conjointe (pièce 25) :

« Mention de l'existence d'images, dépôts de procès-verbaux.

Il existe aussi une possibilité de joindre les images aux procès-verbaux en ISLP. ».

4.7 Gestion des profils et des accès

40. Il ressort de l'analyse que tout le processus est matérialisé grâce à l'interconnexion des différents systèmes. La même analyse des documents transmis ne permet toutefois pas de se faire une image claire et exhaustive de la gestion des profils et des accès. Interrogées à ce sujet (pièce 23), les deux entités de police indiquent dans leur réponse conjointe (pièce 25) (citation littérale, traduction libre) :

« Le premier de chaque mois, il est procédé à une vérification des accès. En cas de sortie de service d'un membre du personnel, ses droits d'accès lui sont retirés. De nouveaux droits d'accès sont octroyés aux nouveaux membres du personnel.

Auprès de la DCA de Flandre orientale, les accès dépendent de badges. Lorsqu'un collaborateur quitte le service, ces droits d'accès lui sont retirés.

Les nouveaux membres du personnel reçoivent une introduction de la part du CP du CIL, lors de laquelle ils reçoivent également des explications concernant la RTI.

Chaque membre de l'équipe RTI dispose d'un identifiant individuel, et les identifiants sont contrôlables puisqu'ils peuvent être consultés auprès de la DRI. ».

41. Il ressort de la visite sur place auprès de la ZP Ninove (pièce 29) que la politique d'accès au *VMS* est liée au grade et à la fonction. Il apparaît aussi que le local où est installé le *VMS* n'est pas pourvu en personnel 24 heures sur 24 et 7 jours sur 7, notamment parce qu'il n'y a que 2 équipes d'intervention. La zone de police a l'intention de porter le nombre d'équipes d'intervention à 3 (en vue de la surveillance du complexe de cellules de la zone), ce qui intensifierait l'occupation du local où se trouve le *VMS* et donc l'utilisation des caméras.

4.8 Délais de conservation des différents systèmes

42. L'analyse du COC a révélé que les délais de conservation appliqués se chevauchent et manquent de clarté : 30 jours, consultation rétrospective des images remontant à 3 heures sur le *VMS*, 48 heures pour le *security desk cam*

[26] Le registre CamELIA permet de consulter les emplacements des caméras de police et les emplacements des caméras de citoyens dont les services de police sont informés. Pour tenir à jour les emplacements des caméras de police dans le registre CamELIA, il est possible de créer, modifier ou supprimer des caméras. La principale plus-value du registre CamELIA est la possibilité qu'il offre de consulter les caméras disponibles de la police et des citoyens dans un seul et même registre.

report et 24 heures pour le script sous-jacent. Interrogées à ce sujet (pièce 23), les deux entités de police apportent dans leur réponse conjointe les précisions suivantes (citation littérale, traduction libre) :

« Images de caméras : 30 jours d'archivage sur le VMS, 3 heures d'accès direct par l'équipe RTI au niveau du VMS.

Pour la communication entre la ZP Ninove et l'équipe RTI, il est recouru à un canal Teams. Après 24 heures et 59 minutes, la ventilation est automatique[27]*. »*.

Lors de la visite sur place auprès de la DCA de Flandre orientale le 30-04-2024 (pièce 30), le COC remarque que le délai de conservation communiqué était erroné : il s'agit de 23 heures, et non 24 comme indiqué. La démonstration des composantes du fonctionnement des différents systèmes (pièces 29 et 30) fait apparaître les différences au niveau des délais de conservation appliqués.

Lors de la visite sur place auprès de la ZP Ninove le 30-04-2024 (pièce 29), il apparaît que l'accès au *VMS* de la ZP Ninove qui est accordé à l'équipe RTI du SICAD de Flandre orientale a été étendu à 12 heures au lieu de 3 heures.

Tant l'AIPD (pièce 7) que les visites sur place (pièces 29 et 30) indiquent qu'en dehors des traitements des images de caméras sur le canal Teams, il n'est procédé à aucun enregistrement externe (dans le cloud) des images[28].

4.9 Fichiers de journalisation du traitement dans son intégralité

43. Étant donné que les traitements visés se matérialisent dans les différents systèmes et composantes, une connaissance du fonctionnement des fichiers de journalisation est indispensable pour pouvoir tracer et documenter un traitement de bout en bout. Les AIPD (pièces 7 et 8) restent cependant très vagues à ce sujet ou abordent les fichiers de journalisation dans des définitions ou termes très généraux. Les aspects suivants ont été explicités lors des visites sur place (pièces 29 et 30) :

- le *VMS* de la ZP Ninove dispose d'une gestion propre du motif de consultation (pièce 29) ;
- les fichiers de journalisation servant à documenter les accès d'une part aux caméras et d'autre part aux *VMS* de la ZP Ninove et de la DCA de Flandre orientale sont gérés par la DRI de la DGR ;
- pour les applications qui n'offrent pas de possibilité propre de spécifier un motif de consultation, le COC a suggéré aux deux entités de police d'examiner si un enregistrement du motif de consultation au niveau de la journalisation centrale en Portal pourrait être une option

4.10 Protocole de protection de la vie privée

44. La pièce 6 transmet en outre un protocole de protection de la vie privée (pièce 9) qui est daté du 07-07-2022 – c'est-à-dire postérieur au traitement et à l'ouverture de l'enquête de contrôle du COC – et qui a été signé par le DirCo de Flandre orientale en date du 11-07-2022. La signature (du chef de corps) de la ZP Ninove est manquante. Interrogées à ce sujet (pièce 23[29]), les deux entités de police indiquent dans leur réponse conjointe (pièce 25) (citation littérale, traduction libre) :

« Protocole 2022 et non 2020.

Lancement du canal Teams le 22/10/2020.

Début du traitement des images (à titre de test) le 07/02/2022. ».

[27] La ventilation automatique doit ici être comprise comme un effacement automatique.
[28] Le fournisseur du *VMS* offre cette possibilité.
[29] La pièce 23 fait erronément mention en son point 1.6 de la date du 07-07-2020. Celle-ci doit évidemment être lue comme « 07-07-2022 ».

Le DOSE constate à nouveau que cette pièce fait systématiquement référence au RGPD, qui ne s'applique pas dans le cadre des traitements opérationnels effectués par la police. Il n'est pas fait directement référence au cadre juridique applicable, à savoir le Titre 2 de la LPD et les articles 25/1 à 25/8 inclus de la LFP[30].

4.11 Utilisation didactique des images de caméras

45. Interrogées (pièce 23) au sujet d'une éventuelle utilisation didactique compte tenu de ce qu'insinue le point 6.3 de la pièce 7 (*« 6.3 Les finalités didactiques et pédagogiques sont autorisées après anonymisation dans le cadre de la formation des membres des services de police. »*), les deux entités de police font savoir dans leur réponse conjointe (citation littérale, traduction libre) :

« Pour les deux parties, la zone de police Ninove et la DCA de Flandre orientale, pas d'application. ».

5 CADRE JURIDIQUE, TECHNIQUE ET FONCTIONNEL

5.1 Introduction

46. Dans l'exposé qui suit, les constatations des conclusions de l'enquête sont confrontées au cadre juridique, technique et fonctionnel en vigueur. Lorsque ce cadre juridique a déjà été expliqué dans d'autres rapports du COC, il y sera fait référence.

Une fois de plus, il s'avère nécessaire de lire conjointement les dispositions des directives ministérielles relatives à la sécurité de l'information, aux accès et aux interconnexions en marge des dispositions légales contenues dans la LPD et la LFP, et de les appliquer dans l'AIPD et les modèles de processus.

5.2 Relation entre les acteurs sur le plan du droit à la protection des données

5.2.1 Référence à un rapport existant

Le COC renvoie ici à son rapport DIO23004[31], et en particulier aux points 40 à 45 inclus du titre 5.6.

5.2.2 Sous-traitant ou fournisseur

47. Additionnellement, le COC souhaite consacrer de l'attention à la distinction entre un sous-traitant et un fournisseur. Pour déterminer si le fournisseur d'un produit ou service est aussi un sous-traitant, il est crucial de vérifier lors de l'analyse des conditions si cette entité externe traite des données à caractère personnel. Si la prestation de services fournie au responsable du traitement se limite exclusivement à la fourniture d'un progiciel, d'une application ou de matériel (serveurs, caméras) ou d'une combinaison de ces éléments, incluant ou non la maintenance, et/ou à la pure fourniture d'un support informatique sans que des données à caractère personnel ne soient inévitablement traitées dans ce contexte, le fournisseur en question n'est pas un sous-traitant[32]. L'accent de la relation se situe alors en effet ailleurs. Même lorsque ce fournisseur, dans les mêmes circonstances que nous venons de décrire, accède soit à distance soit sur site au système pour par exemple exercer des activités de maintenance ou résoudre des incidents, le fournisseur n'est pas un sous-traitant. Dans ces cas, il n'est donc pas nécessaire de conclure une convention de traitement des données. **En revanche, il est alors vivement recommandé de conclure une clause de confidentialité ou un**

[30] Le 07-07-2022, il n'était pas encore question de l'article 25/9 de la LFP, qui a été inséré par la loi du 19-10-2023.
[31] Rapport DIO23004 du 25 avril 2024 du contrôle restreint de l'Organe de contrôle de l'information policière dans le cadre de sa compétence de surveillance et de contrôle concernant le recours à une caméra mobile montée sur un drone dans le cadre de l'appui interzonal, non publié, disponible sur le *Sharepoint* de la GPI, Page REGPOL, https://bpolb.sharepoint.com/sites/regpol/Publications%20COC%20%20Publicaties%20COC/Forms/AllItems.aspx.
[32] Voir Comité européen de la protection des données, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, version arrêtée le 7 juillet 2021, p. 31-32 *in fine*.

NDA[33]. En effet, on ne saurait exclure l'éventualité que le fournisseur, dans le cadre de la réalisation des tâches convenues, soit confronté accidentellement – mais pas structurellement (intentionnellement) – à des données policières. Il convient ici également de mettre en garde contre les situations dans lesquelles le responsable du traitement est trop dépendant du fournisseur et n'est donc pas en mesure d'en changer sans s'exposer à des frais substantiels[34].

5.3 Interconnexion (partage) de données policières

5.3.1 La directive ministérielle relative aux interconnexions

48. La directive ministérielle relative aux interconnexions[35] définit l'interconnexion comme une forme de traitement de données au sens de l'article 26, 2° de la LPD, qui permet de partager des données entre des personnes qui en ont besoin dans le cadre de leurs missions légales. L'interconnexion permet en outre d'apporter une plus-value aux données initialement traitées en les corrélant et en les enrichissant. Le partage et l'enrichissement de données policières (informations et données à caractère personnel) sont une donnée de base pour une fonction de police guidée par l'information, et l'interconnexion de banques de données devrait être la règle de la gestion des informations policières opérationnelles, basée sur une gestion adéquate et différenciée des profils et des accès (voir le titre 4.4.).

Concrètement, cette directive peut être matérialisée par les actions suivantes :

1) la possibilité via une seule recherche de consulter des données qui, originellement, sont traitées dans différentes banques de données et qui sont dès lors dispersées ;
2) la possibilité de réaliser des corrélations de données qui sont traitées originellement dans différentes banques de données, ou d'établir des liens entre ces données, à l'aide d'outils d'analyse ou d'applications d'analyse ou, le cas échéant, de listes ou d'extraits, mais en tenant compte de la nécessité et de la proportionnalité en mettant en œuvre des mesures techniques et organisationnelles appropriées ;
3) la possibilité d'enrichir les données en alignant des sources internes et externes de référence.

Les conditions et modalités suivantes s'appliquent :

1) la pertinence des données en marge du besoin d'en connaître du profil, ainsi que l'état de maturité, la formation et l'expérience de ce dernier (voir aussi le titre **Fout! Verwijzingsbron niet gevonden.**) ;
2) la clarté concernant l'état de validation des données ;
3) la catégorie de personnes concernées dont relève la personne enregistrée dans les banques de données policières opérationnelles doit être identifiable de manière non ambiguë (auteur, victime, témoin, …) ;
4) à moins que cela ne soit excessif, une consultation préalable ou simultanée de la BNG, laquelle doit aussi être alimentée correctement ;
5) le respect des règles d'accès et des délais de conservation ;
6) l'identification de l'origine des données (transparence) ;
7) l'enregistrement du traitement en RegPol ;
8) l'actualisation des données conformément à l'article 44/5 §6 de la LFP (et par extension en application de l'article 646 du Code d'instruction criminelle) ;
9) la présence de fichiers de journalisation, incluant le motif de consultation ;
10) les outils et applications d'analyse doivent pouvoir être audités ;
11) la mise en place d'une politique prévoyant des contrôles systématiques et proactifs de l'utilisation et/ou de la consultation des banques de données policières.

La manière dont ces actions, conditions et modalités sont mises en œuvre doit dès lors être exposée dans l'AIPD.

[33] *Non Disclosure Agreement* : convention par laquelle les parties concernées conviennent de garder certaines informations secrètes et de ne donc pas les partager avec d'autres parties.
[34] *Vendor lock-in* (enfermement propriétaire) et *path-dependency*.
[35] Directive contraignante commune des ministres de la Justice et de l'Intérieur du 4 août 2021 relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles 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.

5.3.2 Interconnexions dans le cadre du processus des traitements de caméras effectués par la police

49. Le COC souhaite renvoyer aux recommandations qu'il a formulées précédemment dans le cadre d'une gestion efficace et intégrée de l'utilisation policière de caméras[36].

5.3.3 Le rôle de *MS Teams* dans les interconnexions dans le cadre du processus des traitements de caméras effectués par la police

50. *MS Teams* joue un rôle tant dans le traitement effectué par la DCA de Flandre orientale et la ZP Ninove que dans le modèle vidéo fonctionnel (pièce 17). Pour la DCA de Flandre orientale et la ZP Ninove, *MS Teams* sert de canal pour mettre rapidement des images et des photos à la disposition des équipes sur le terrain. Selon le modèle vidéo fonctionnel (pièce 17) et la réponse de l'Appui aérien de la DGA (DAFA) (pièces 20 et 22), le rôle de *MS Teams* se limite essentiellement à la possibilité de consulter les images en temps réel au moyen d'un partage d'écran, et ce lors de pannes techniques ou lorsqu'il n'y a pas d'alternative. Les réponses de la DGA/DAS (pièce 21) révèlent un besoin similaire en faisant référence à la plus-value constatée lors de tests en « situation réelle ». De plus, il apparaît que *MS Teams* intéresse également d'autres entités de police qui ont besoin de pouvoir transmettre des fichiers volumineux contenant des traitements d'images à un utilisateur final[37].

À aucun moment *MS Teams* ne semble jouer un rôle en tant que moyen de captation (le cas où un fonctionnaire de police individuel utilise la caméra de son smartphone pour recueillir des images et les transmettre à un *VMS*) ou en tant que moyen de réception – hormis au moyen d'un partage d'écran – d'images de caméras. Autrement dit, *MS Teams* ne semble pas non plus être sur ce plan une condition sine qua non à la création d'un modèle vidéo fonctionnel.

51. Le modèle vidéo fonctionnel (pièce 17) fait toutefois référence à des alternatives qui pourraient répondre aux besoins détectés de suivre des événements en temps réel, ainsi qu'au besoin de consulter les images par la suite, sans parler d'une éventuelle intégration avec les possibilités de la plateforme FOCUS. La question à se poser est donc de savoir s'il existe encore, après l'application de ce modèle vidéo fonctionnel, une nécessité d'utiliser *MS Teams* dans le cadre des traitements policiers, en particulier sur le plan des interconnexions. Il convient ici de faire remarquer qu'un rapport de 2022[38] (pièce 31) du ministère néerlandais de la justice et de la sécurité consacré à l'utilisation de l'application *MS Teams* épingle 7 risques faibles et 1 risque élevé. Le risque élevé a trait à l'accès potentiel des services de recherche et de renseignement américains à des données à caractère personnel très sensibles et particulières, de sorte qu'il est conseillé de ne pas utiliser *MS Teams* (ni par extension *Sharepoint/OneDrive*) pour échanger des fichiers sensibles, à moins de les crypter au préalable au moyen de clés détenues en gestion propre. Il est par ailleurs recommandé de ne pas échanger d'informations sensibles lors de réunions/d'appels en ligne (*Teams/Streams*). Sans préjudice des risques identifiés inhérents à l'utilisation tout particulièrement de *MS Teams*, Microsoft n'a notamment pas encore prévu de *end-to-end-encryption* (E2EE) pour les réunions en *MS Teams*. En d'autres termes, les 'enregistrements'[39] des réunions (réunions collectives et messagerie instantanée) sont disponibles en clair sur les serveurs de Microsoft.

Une étude subséquente de la même source[40] (pièce 32) indique que Microsoft a pris des mesures pour atténuer six risques élevés, mais que les organisations ne peuvent pas utiliser ces services dans le cloud pour l'échange ou le stockage de données à caractère personnel sensibles et particulières. Elles n'y sont autorisées que si elles sont en mesure de crypter le contenu au moyen de clés propres. Cette mise en garde est due au risque élevé d'accès potentiel à ces données par des acteurs américains. Ce risque subsiste en dépit du fait que Microsoft traite – ou du moins affirme traiter – (contractuellement) pour ainsi dire toutes les données à caractère personnel de ses clients professionnels européens exclusivement dans des centres de données établis en Europe[41].

[36] CON20004, DIO20009/1, DIO23004.
[37] DIO23004 (non publié).
[38] *DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021), Data protection impact assessment on the processing of Diagnostic Data*, version 1.1, Ministerie van Justitie en Veiligheid, 16-02-2022.
[39] On entend par 'enregistrements' l'image et le son, les fichiers utilisés et les conversations de messageries instantanées, les métadonnées, …
[40] https://www.privacycompany.eu/blogpost-nl/nieuwe-dpia-voor-de-rijksoverheid-en-universiteiten-op-microsoft-teams-onedrive-en-sharepoint-online.
[41] Comme indiqué au point 13 des mesures de sécurisation minimales imposées par la directive ministérielle du 13.07.2021 relative à la sécurité de l'information.

En combinaison avec les incertitudes quant à la gestion des utilisateurs et aux fichiers de journalisation et avec les nombreuses possibilités d'accorder l'accès également à des parties externes à l'organisation selon une procédure simple et de partager des fichiers, il en découle que l'utilisation de *MS Teams* ne peut pas être considérée comme exempte de risques. Une décision du CEPD[42] du 8 mars 2024 visant à prendre une mesure correctrice à l'encontre de la Commission européenne dans le sillage de la violation de plusieurs règles en matière de protection des données lors de l'utilisation d'applications de Microsoft rejoint ce point de vue. Bien que l'utilisation de solutions de Microsoft devienne de plus en plus une pratique standard au sein de la GPI, il faudra en permanence en contrôler la compatibilité avec le droit à la protection des données en vigueur. Sans parler du contexte géopolitique actuel et des risques qui découlent dans ce cadre également de l'utilisation (exclusive) d'applications *'big tech'* ou GAFAM[43] (américaines).

5.3.4 Travail hybride[44]

51. La police intégrée n'échappe pas à l'évolution de la société vers le travail hybride, à savoir une forme de travail consistant à travailler en partie à distance, par exemple à domicile, et en partie sur le lieu de travail physique, à savoir dans un bureau de police ou sur le terrain. Il va de soi que les collaborateurs doivent pour ce faire utiliser des appareils – radios, ordinateurs portables, smartphones ou tablettes – qui appartiennent au membre du personnel ou qui sont mis à sa disposition par l'organisation, ainsi que des canaux d'accès comme des réseaux fixes ou mobiles sur site ou sur le lieu de travail, des *hotspots*, des connexions VPN, etc. … Lorsqu'une organisation opte pour une approche *BYOD*, il doit exister une politique détaillée à ce sujet réglant notamment l'aspect de la sécurisation et prévoyant les mesures que le collaborateur doit prendre. Les collaborateurs doivent savoir clairement ce qu'ils peuvent, mais surtout ce qu'ils ne peuvent pas faire avec leurs appareils. Une telle politique ne peut en aucun cas être imposée unilatéralement, avec par exemple la diffusion de données personnelles des collaborateurs (numéros privés, adresses e-mail privées, etc. …). Nous ne nous étendrons pas davantage sur la problématique de la pratique *BYOD* dans le présent rapport.

5.4 Accès aux données policières

5.4.1 La directive ministérielle relative aux accès

52. La directive ministérielle relative aux accès[45] met en avant le principe *« need to know »* pour l'octroi des accès à la BNG, aux banques de données de base, aux banques de données techniques et aux banques de données particulières. Les membres des services de police sont identifiés et authentifiés avant chaque accès aux banques de données et aux données qu'elles contiennent, et chaque accès est journalisé. Les chefs de corps, pour la police locale, et le commissaire général, les directeurs généraux et les directeurs, pour la police fédérale, décident pour les membres de leur personnel quels accès sont nécessaires pour exécuter les tâches qu'ils leur confient et définissent à ce sujet une politique d'accès,

[42] Le Contrôleur européen de la protection des données, en anglais *EDPS* pour *European Data Protection Supervisor*, est l'autorité de contrôle indépendante qui veille à ce que les institutions et organes européens respectent le droit à la protection de la vie privée et à la protection des données lorsqu'ils traitent des données à caractère personnel et définissent de nouvelles lignes politiques.

[43] **G**oogle, **A**pple, **F**acebook (actuellement Meta), **A**mazon et **M**icrosoft.

[44] Auquel on peut ajouter les pratiques *BYOD*, *CYOD* et *COPE* :
- *BYOD* : *Bring Your Own Device* : le collaborateur utilise sur une base volontaire ses propres appareils. La sécurisation n'est pas uniforme, dépend de l'utilisateur et est de ce fait souvent moins bien garantie ; l'appareil est également utilisé à des fins privées et la gestion des appareils est (plus) complexe pour l'organisation.
- *CYOD* : *Choose Your Own Device* : le collaborateur peut faire son choix parmi une offre (restreinte) d'appareils qui appartiennent à l'organisation. La sécurisation relève de la responsabilité de l'organisation et est souvent meilleure. L'appareil ne peut PAS être utilisé à des fins privées et la gestion des appareils est moins complexe pour l'organisation.
- *COPE* : *Company issued Personally Enabled* : l'organisation prévoit des appareils que les collaborateurs peuvent également utiliser à des fins privées. La sécurisation relève de la responsabilité de l'organisation et est souvent meilleure. L'appareil peut être utilisé à des fins privées et la gestion des appareils est moins complexe pour l'organisation.

[45] Directive commune contraignante des ministres de la Justice et de l'Intérieur du 13 juillet 2021 relative aux règles d'accès des membres des services de police à la banque de données nationale générale, aux banques de données de base, particulières et techniques.

qui reflète les règles prescrites et qui correspond à la situation locale dont ils sont responsables. Pour déterminer si l'accès à une banque de données est nécessaire, les mandataires susmentionnés s'appuient notamment :

1) sur les finalités définies dans la LFP pour la banque de données en question ;
2) sur les catégories de personnes visées à l'article 44/5 de la LFP ;
3) sur le niveau d'évaluation des données ;
4) sur le niveau de validation des données ;
5) sur le profil requis pour y accéder ;
6) sur les droits d'accès et ce qu'ils permettent.

Une attention particulière est requise lorsqu'il s'agit d'accorder un accès à des données à caractère personnel relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé ou à la vie ou l'orientation sexuelle et lorsque des données génétiques ou biométriques sont traitées.

Il convient par ailleurs de faire une distinction entre un accès permanent et un accès temporaire.

La directive souligne également l'importance d'un niveau de connaissances approprié.

La gestion des accès est de préférence supportée par un système de permissions basé sur des rôles servant de registre central des profils et des accès, étant entendu que des exceptions sont prévues pour les banques de données particulières et les banques de données techniques locales. La gestion des accès est un processus dynamique avec des mises à jour régulières de sorte que seuls les accès nécessaires soient actifs. Ce point doit être contrôlé au moins une fois par an.

L'identification, l'authentification et la journalisation, y compris l'obligation de prévoir une authentification multifacteur (MFA), sont des éléments essentiels de la gestion des accès.

5.4.2 Application au cas examiné : les accès au sein d'un système complexe de traitements de caméras interconnectés

53. Partant de la réglementation en vigueur et de l'hypothèse qu'un *VMS* doit être considéré comme une banque de données particulière, la gestion des accès pour la diversité des systèmes en présence dans le cas qui nous occupe mais en particulier dans le cadre du modèle vidéo fonctionnel (pièce 17) semble complexe. Bien que la directive ministérielle relative aux interconnexions autorise l'interconnexion de banques de données particulières, une gestion des accès, si elle doit chaque fois être réglementée à partir d'un registre local – voire si elle est gérée par un seul fournisseur – n'est pas une sinécure, en particulier dans un concept comme celui décrit par le modèle vidéo fonctionnel (pièce 17), sans parler d'une reconstitution *end-to-end* d'un traitement à partir des fichiers de journalisation. Une gestion centrale de tels accès et une journalisation centrale *end-to-end* des traitements s'imposent. Le COC fait à cet égard référence notamment à l'application du principe AAA (authentification, autorisation et accounting) dans le cadre :

- du rôle de toute une série de systèmes de gestion comme LDAP, PolBacc, ACC, LORI, Active Directory et de leurs relations mutuelles dans le contexte du registre central des profils et des accès tel que visé au point III de la directive ministérielle susmentionnée du 13-07-2021 ;
- du rôle de la source pour la gestion du personnel de la police intégrée et la manière dont ce rôle se matérialise dans les services individuels de la police fédérale ou des zones de la police locale ainsi que les processus dérivés comme le registre téléphonique CRC et les adresses e-mail police.belgium.eu ;
- de la gestion des accès au sein même d'une application ;
- de la distinction entre les collaborateurs internes à la GPI (Ops/CaLog) et les collaborateurs externes à la GPI ainsi que toutes les parties externes qui utilisent des informations de la police[46].

[46] Par exemple en application de l'article 25/5 §2 de la LFP pour la gestion d'événements d'envergure ou d'incidents inattendus qui font l'objet d'une prise en charge multidisciplinaire dans le cadre de la planification de crise et d'urgence.

54. Dans l'environnement policier actuel, la transmission ultérieure de données sur des supports externes semble encore inévitable. Les responsables du traitement (fonctionnels) doivent donc prendre les mesures techniques et organisationnelles nécessaires pour gérer cette réalité. Dans un tel contexte, le risque de transmission incontrôlée de données est grand et le contrôle est difficile. Ce risque pourrait être atténué :

- sur le plan organisationnel en déterminant (de manière limitative) dans quelles circonstances des supports externes peuvent être utilisés ;
- sur le plan technique en recourant au cryptage des données sur le support.

5.5 Les analyses d'impact et de risques

5.5.1 Types d'analyses d'impact et de risques

55. Le COC renvoie à ce sujet à son rapport DIO23004 susmentionné[47], et en particulier aux points 34-36 du titre 5.3.

5.5.2 Une AIPD de référence pour des traitements similaires

56. Le COC renvoie à ce sujet à son rapport DIO23004 susmentionné, et en particulier au point 37 du titre 5.3.

5.5.3 Application au cas examiné : évolution vers des AIPD de référence pour les traitements de caméras effectués par la police

57. Les imprécisions initiales relevées lors de la première analyse des pièces 7 à 11 incluse, lues conjointement avec certaines des réponses reçues dans la pièce 25 prouvent que l'établissement d'une AIPD est un exercice complexe qui requiert une connaissance approfondie des aspects juridiques, techniques et fonctionnels ainsi qu'une bonne coordination entre les acteurs impliqués dans ce processus. Vu le modèle vidéo fonctionnel de la GPI (pièce 17) et la complexité de l'établissement de telles analyses, il semble également préférable en la matière d'établir une seule AIPD de ce modèle fonctionnel, par exemple au niveau national, qui servira à évaluer les projets partiels visant à évoluer vers ce modèle, comme celui qui nous occupe, en combinaison ou non avec une AIPD de référence correspondante mais réduite.

5.6 Registres

58. La loi du 19 octobre 2023 a également modifié l'article 25/8 de la LFP et il n'est plus question désormais d'un registre local inventoriant toutes les utilisations de caméras. Il est à présent prévu que tous les traitements relatifs à l'usage des caméras doivent être tenus à jour dans le registre unique des activités de traitement des services de police visé à l'article 145 de la LPI (RegPoL), de sorte que le recours à la vidéosurveillance peut dans le même temps être vérifié en fonction du registre des activités de traitement. Le registre reprenant la géolocalisation doit également être tenu à jour. Le COC est d'ailleurs d'avis qu'il pourrait y avoir une plus-value opérationnelle à mettre en place une synchronisation entre ce registre unique de géolocalisation CamELIA d'une part et le système *CAD* d'autre part ou, par extension, entre le registre unique de géolocalisation CamELIA et toute autre application policière fonctionnant avec des emplacements de caméras.

5.7 Test d'applications policières

[47] Rapport DIO23004 du 25 avril 2024 du contrôle restreint de l'Organe de contrôle de l'information policière dans le cadre de sa compétence de surveillance et de contrôle concernant le recours à une caméra mobile montée sur un drone dans le cadre de l'appui interzonal, non publié, disponible sur le *Sharepoint* de la GPI, Page REGPOL, https://bpolb.sharepoint.com/sites/regpol/Publications%20COC%20%20Publicaties%20COC/Forms/AllItems.aspx.

59. À titre subsidiaire, l'une des réponses aux différentes questions (pièce 21) fait à nouveau apparaître le besoin de pouvoir tester le bon fonctionnement des applications policières. Au surplus, le COC doit ici faire référence à ses conclusions antérieures[48,49] selon lesquelles le traitement d'informations et de données à caractère personnel policières à des fins de test, dans une phase expérimentale, devrait être réglementé afin de mettre en place un cadre juridique clair et cohérent.

5.8 Utilisation didactique des images de caméras

60. L'utilisation d'images à des fins didactiques telle que prévue à l'article 25/7 §2 de la LFP est une finalité différente étant donné qu'elle est explicitement limitée aux fins didactiques et pédagogiques dans le cadre de la formation des membres du cadre opérationnel ou logistique des services de police, qui plus est après anonymisation.

6 APPLICATION DES CONSTATATIONS AU CAS EXAMINÉ ET AU MODÈLE VIDÉO FONCTIONNEL À LA LUMIÈRE DE LA VISION DU COC – SUGGESTIONS EN VUE D'UNE OPTIMALISATION FUTURE AU SEIN DE LA GPI

6.1 Introduction

61. L'examen de la conformité au cadre fonctionnel, technique et réglementaire du cas concret des traitements de caméras effectués par la DCA de Flandre orientale pour la ZP Ninove à la lumière de la vision intégrée de l'utilisation des caméras de police que le COC avait déjà exposée précédemment – et ce, en marge du modèle vidéo fonctionnel qui est en train d'être déployé au sein de la GPI – nous amène à formuler plusieurs suggestions d'optimalisation future au sein de la GPI. Ces suggestions ne sont évidemment pas contraignantes et doivent donc être considérées comme une invitation à poursuivre l'analyse et la réflexion.

Le COC a été dans le cas présent confronté à une initiative prise par une entité d'appui fédérale et une police locale en vue de pouvoir offrir un bon appui opérationnel à certaines opérations de la police locale en utilisant des moyens existants et disponibles dans un contexte caractérisé par des budgets d'investissement limités. Il se crée de cette manière une culture de solutions (supra)locales et ponctuelles créatives permettant de répondre à un besoin opérationnel légitime. Pourtant, il existe un modèle conceptuel défendable qui, en raison des limitations d'ordre budgétaire, ne peut toutefois pas être déployé pleinement. Il va de soi que cette situation soulève un certain nombre de questions plutôt importantes, comme celle du rôle des responsables du traitement, des sous-traitants et des fournisseurs, de l'établissement d'une AIPD complexe, des interconnexions de systèmes et de la gestion des accès (y compris l'autorisation, l'authentification et l'audit). La résolution de ces questions requiert des connaissances juridiques, techniques et fonctionnelles qui dépassent régulièrement le niveau de connaissances des acteurs directement impliqués et qui nécessitent une approche coordonnée et de préférence nationale. L'obligation légale imposée par la LFP de continuer à lier les traitements policiers à des banques de données ne fait qu'ajouter à cette complexité.

Ces suggestions dépassent par conséquent les constatations proprement dites du présent rapport ainsi que la responsabilité individuelle du chef de corps et du directeur concernés et requièrent plutôt une approche à l'échelle de la GPI de l'application du droit à la protection des données dans le contexte policier dans le cadre de la gestion des accès et de l'interconnexion de systèmes entre les différents services et zones de police de la police locale et de la police fédérale. Les suggestions qui suivent sont dès lors adressées aux responsables politiques de tous les niveaux, y compris les ministres de tutelle.

[48] Recommandation n° 2 du rapport de contrôle DIO21006 du 4 février 2022 de l'Organe de contrôle de l'information policière relatif à l'utilisation de l'application *Clearview AI* par la police intégrée.
[49] Recommandation n° 3 du rapport DIO23001 du 2 mai 2023 du contrôle restreint de l'Organe de contrôle de l'information policière dans le cadre de sa compétence de surveillance et de contrôle concernant des infractions commises par des membres de la GPI dans le cadre de traitements dans la BNG.

6.2 Normalisation des traitements policiers, pas nécessairement des banques de données policières

62. Ni la *LED* ni la LPD n'exigent la création de banques de données policières. Ces textes mettent en effet l'accent sur la légalité, la nécessité et la proportionnalité des 'traitements', sur les finalités et sur les (catégories de) données à caractère personnel, et pas *ab initio* sur le support ou le système de traitement en lui-même[50]. La création d'une banque de données est plutôt un choix pragmatique. Néanmoins, la LFP détermine de manière restrictive les banques de données à créer et les types de données à caractère personnel à traiter dans ces banques de données. Pour que la conservation (et l'utilisation) des données à caractère personnel soi(en)t licite(s), les données à caractère personnel doivent donc pouvoir être attribuées à une banque de données policière déterminée. À cet égard, cela implique dans une certaine mesure une restriction des traitements effectués par la police, comme le cas examiné ici l'illustre abondamment. S'accrocher au concept des banques de données ne semble avoir d'utilité que lorsque la banque de données en question a une finalité à part entière, comme le Registre national ou la Banque-Carrefour des véhicules. Une opportunité devrait d'ailleurs apparemment se présenter, dès lors que l'accord de gouvernement pour la période 2025-2029 (chapitre *« Sécurité »*, section *« Recherche et partage d'informations »*) avance spécifiquement la piste législative : *« À la suite de la directive européenne 2016/680, la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a déjà prévu la transposition de cette directive pour l'application spécifique qu'est le traitement de données à caractère personnel par les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales ou l'exécution de peines. La description des traitements eux-mêmes est aujourd'hui réglée par la loi du 5 août 1992 sur la fonction de police et le code de procédure pénale.* ***Dans une prochaine étape, un cadre juridique sera créé par une loi spécifique sur les données de police*** *afin de fusionner ces matières. Cette loi réglementera les droits et obligations de la police et des citoyens en ce qui concerne le traitement des données policières. … ».*[51]

6.3 Choix pour la détermination de la relation juridique entre les responsables du traitement (fonctionnels), le sous-traitant et le fournisseur

63. La relation opérationnelle qui existe entre le SICAD de Flandre orientale en tant qu'unité d'appui, d'une part, et la ZP Ninove qui bénéficie de l'appui, d'autre part, ne semble pas pouvoir être transposée automatiquement aux responsabilités qui sont définies dans le droit à la protection des données. D'une part, les missions et les compétences sont définies dans la LPI, et en particulier à l'article 104*bis*, ainsi que dans l'arrêté royal du 26 juin 2002[52]. D'autre part, il s'agit de traitements qui, par la volonté du législateur, sont effectués dans les banques de données policières. Pour les traitements de caméras effectués par la police, la LFP désigne comme suit les responsables du traitement :

- l'article 25/5, qui fait référence aux articles 7 à 7/3 inclus de la LFP et qui désigne donc le chef de corps ou le directeur coordonnateur ;
- l'article 44/11/3*sexies*, qui a toutefois uniquement trait aux banques de données techniques, lesquelles se limitent selon l'article 44/2 aux caméras intelligentes et aux systèmes visant la reconnaissance automatique des plaques d'immatriculation, et qui désigne soit le chef de corps (pour les banques de données techniques locales), soit les ministres de l'Intérieur et de la Justice (pour les banques de données techniques nationales) en tant que responsables du traitement.

Vu la logique appliquée par le législateur qui consiste à faire effectuer les traitements de données policiers dans des banques de données, et en l'absence d'une description claire du type de banque de données qu'est un *VMS*, seul l'article 44/11/3 de la LFP semble donc pouvoir être invoqué comme fondement juridique pour les banques de données dans

[50] Cf. R. SAELENS, « De Wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie », dans F. GOOSSENS, K. DE PAUW, F. VERSPEELT (éd.) *De sluier rond anonimiteit opgelicht … Identiteits-, privacy- en persoonsgegevensafscherming in het strafprocesrecht en politierecht*, die Keure 2022, 316-318.

[51] Accord de coalition fédérale 2025-2029, p. 135, https://www.belgium.be/sites/default/files/resources/publication/files/Accord_gouvernemental-Bart_De_Wever_fr.pdf.

[52] Arrêté royal du 26 juin 2002 concernant l'organisation des centres de dispatching centralisés et du point de contact national, *M.B.* 15 août 2002.

lesquelles des traitements de caméras sont effectués. En ce sens, il semble qu'il pourrait être question pour la communication *VMS* (to *VMS*) d'une relation de *« responsables conjoints du traitement »* d'un traitement de données à caractère personnel effectué dans une banque de données particulière au sens de l'article 44/11/3 de la LFP. Cette vision semble en tout cas être corroborée par un arrêt de la Cour de Justice de l'Union européenne[53], dans lequel la Cour souligne qu'il n'est même pas nécessaire qu'il existe un régime légal entre deux entités quant aux finalités et aux moyens du traitement pour que celles-ci puissent être considérées comme des responsables conjoints du traitement. Les chefs de corps concernés doivent dans ce contexte définir de manière transparente, par voie d'accord entre eux, leurs responsabilités respectives pour le respect des obligations. Toutefois, l'existence d'un tel accord constitue non pas une condition préalable pour que deux entités ou plus soient (ou puissent être) qualifiées de *« responsables conjoints du traitement »*, mais une obligation que la *LED*/la LPD impose aux responsables conjoints du traitement, une fois qualifiés de tels, aux fins d'assurer le respect des exigences de la LPD et de la LFP pesant sur eux. La responsabilité conjointe ne sous-entend pas nécessairement une responsabilité équivalente des chefs de corps concernés à l'égard du traitement conjoint. Chaque chef de corps concerné peut être impliqué à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte des circonstances concrètes du traitement.

Par ailleurs, il convient de déterminer le rôle exact de certaines tierces parties. S'agit-il de sous-traitants ou de fournisseurs ? Dans le cas qui nous occupe, les responsables du traitement fonctionnels semblent avoir à ce sujet pour les parties du processus et les systèmes et outils utilisés une vision différente de celle de la DRI, et ce en dépit de l'existence d'une note à ce sujet au niveau du corps. Un fournisseur ne peut pas non plus être considéré comme un sous-traitant lorsqu'il n'est pas question d'un traitement de données à caractère personnel, mais uniquement d'une prestation de services. La complexité de l'application dans la structure mise en place par la DCA de Flandre orientale et la ZP Ninove montre que certains aspects doivent à cet égard être examinés au niveau du modèle vidéo fonctionnel de la GPI étant donné que la multitude d'entités et de systèmes impliqués en fait une donnée beaucoup plus complexe. Au surplus, le COC rappelle qu'il s'agit d'une suggestion s'assortissant d'une invitation à approfondir l'analyse, et donc pas d'une prise de position définitive.

6.4 Interconnexion de systèmes

64. La GPI utilise actuellement une multitude de systèmes, de plateformes et d'applications aux possibilités et finalités similaires. Dans ce contexte, le rôle exact des applications O365 GPI pour les traitements policiers *sensu lato* n'est pas toujours très clair, et il est difficile d'évaluer à quel point la GPI évolue vers des situations de (quasi) enfermement propriétaire[54]. Le modèle vidéo fonctionnel (pièce 17) offre suffisamment de possibilités de conserver les traitements d'images au sein des systèmes propres sans devoir faire appel à des parties externes. La GPI va devoir poser un choix quant au rôle exact que les applications O365 GPI doivent jouer – en commençant d'ailleurs par décider si elles doivent vraiment jouer un rôle – compte tenu des systèmes propres qui existent et en particulier de FOCUS, et établir les responsabilités qui découlent de ce choix au niveau du responsable du traitement (fonctionnel), du sous-traitant et du fournisseur (voir le titre 6.3 ci-dessus).

6.5 Gestion des accès

65. La diversité des systèmes de gestion comme LDAP, PolBacc, ACC, LORI, Active Directory et même de la gestion des accès dans certaines applications et de leurs relations mutuelles complique la mise en place d'une gestion des accès au sens de la directive ministérielle. Si l'on ajoute à cela la diversité des systèmes qui existent pour la gestion des fichiers de journalisation, voire leur absence (par exemple dans *MS Teams*), dans le cadre du contrôle du rôle joué par

[53] Cf. CJUE 5 décembre 2023, C-683/21, considérants 41 – 45.
[54] Le concept d'enfermement propriétaire, désigné en anglais par le terme *vendor lock-in*, fait référence à la situation dans laquelle un client est dépendant d'un fournisseur pour certains produits et/ou services du fait qu'il n'est pas en mesure de changer de fournisseur sans s'exposer à des frais substantiels ou à des désagréments (opérationnels).

les fournisseurs/sous-traitants, on ne peut que constater que la gestion et l'audit des accès doivent d'urgence être mis en conformité avec les directives ministérielles en ce qui concerne :

- le rôle de la source pour la gestion du personnel de la police intégrée et la manière dont ce rôle se matérialise dans les services individuels de la police fédérale ou des zones de la police locale ainsi que les processus dérivés comme le registre téléphonique CRC et les adresses e-mail police.belgium.eu ;
- la gestion des accès au sein même d'une application ;
- la distinction entre les collaborateurs internes à la GPI (Ops/CaLog) et les collaborateurs externes à la GPI ainsi que toutes les parties externes qui utilisent des informations de la police ;
- le contrôle et l'audit de ces aspects.

Spécifiquement en ce qui concerne *MS Teams*, le COC constate que la ZP Ninove et la DCA de Flandre orientale sont conscientes de l'absence de fichiers de journalisation et sont déterminées à y travailler en collaboration avec la direction compétente.

Le COC invite donc les parties concernées à poursuivre leurs efforts pour éclaircir ce point et y remédier.

6.6 Analyses d'impact et de risques – réutilisation des analyses d'impact relatives à la protection des données

66. En dépit de la suppression de l'autorisation de principe des Conseils communaux pour l'utilisation de caméras mobiles (cf. l'article 25/4 §6 de la LFP) par les services de police, il convient toujours de réaliser dans le contexte de l'utilisation de caméras par la police des analyses d'impact et de risques tant au niveau opérationnel qu'au niveau de la protection de la vie privée. Cette dernière précise également pour chaque type de caméras mobiles les finalités en vue desquelles les caméras seront installées et utilisées, ainsi que les modalités de leur utilisation. Si une analyse d'impact relative à la protection des données doit être réalisée conformément à l'article 58 de la LPD, il va de soi que le même document pourra également être utilisé pour ce faire.

Il est important de souligner que le but d'une analyse d'impact et de risques au niveau de la protection de la vie privée telle que prévue par la LFP[55] ou d'une AIPD telle que prévue par la LPD[56] n'est **pas** de décrire ou d'analyser des aspects purement opérationnels en fonction des risques, et encore moins de soumettre de telles informations au Conseil communal si la loi le prévoit. Dans le cadre de la demande d'autorisation, le législateur stipule clairement que celle-ci doit être basée sur une analyse d'impact et de risques. En d'autres termes, il s'agit d'un exercice de réflexion sur les principes de proportionnalité et de subsidiarité, et la réalisation de cette analyse permettra de définir clairement les finalités et les catégories de données traitées. Le responsable du traitement pourra ainsi également évaluer le type de caméras et le délai de conservation nécessaires pour atteindre les objectifs opérationnels. Lorsque le responsable du traitement a réalisé cet exercice et que la loi exige qu'une demande d'autorisation préalable de principe soit adressée à l'autorité compétente, il est suffisant de communiquer *in abstracto* les résultats de cette analyse à cette autorité compétente, de sorte que d'une part, rien ne s'oppose à cette divulgation mais que d'autre part, aucun élément opérationnel, tactique ni stratégique n'est rendu public.

Par ailleurs, il est prévu qu'une seule analyse d'impact relative à la protection des données puisse être utilisée pour évaluer plusieurs traitements comparables en termes de nature, d'envergure, de contexte, de finalité et de risques. Cette solution peut certainement être envisagée dans le cas qui nous occupe, qui vise l'implémentation, éventuellement partielle, d'un modèle vidéo fonctionnel à l'échelle de la GPI, soit au niveau national, soit par arrondissement.

6.7 Test de traitements policiers – nécessité sans cadre légal

[55] Article 25/4 §2 de la LFP.
[56] Article 58 de la LPD.

67. Le COC comprend bien la situation particulière créée par la combinaison des développements nécessaires et du test de ces développements dans un contexte de traitements policiers. Les normes ISO27K qui sont applicables en la matière en vertu de la loi[57] stipulent que l'environnement de développement, l'environnement de test et l'environnement opérationnel doivent être séparés (*« development, test and operational environments must be separated »*). *Hic et nunc*, le COC ne peut que constater l'absence d'un cadre réglementaire régissant l'utilisation de données opérationnelles pour le développement et le test de nouveaux systèmes de traitement de données dans un contexte de traitements relevant de la police administrative et judiciaire, mais il comprend en l'occurrence tout à fait la nécessité de ces opérations. Une initiative législative en la matière est également une nécessité et commence à devenir urgente vu l'imminence de la mise en œuvre complète du Règlement sur l'intelligence artificielle (*AI Act*[58]).

6.8 En résumé

68. Pour résumer, l'Organe de contrôle suggère, pour les traitements d'images de caméras effectués par la police :

- de plancher sur la mise au point d'un cadre normatif partant des traitements policiers et pas nécessairement des banques de données policières ;
- de définir les relations entre les différents acteurs, à savoir le responsable du traitement (fonctionnel), le sous-traitant et le fournisseur en ce qui concerne la responsabilité des traitements ;
- d'utiliser effectivement comme normes les directives ministérielles adoptées en exécution des dispositions de l'article 44/4 de la LFP et de mettre les traitements en conformité avec ces directives, notamment dans le cadre du modèle vidéo fonctionnel ;
- d'étudier la piste de la réutilisation d'analyses d'impact relatives à la protection des données par plusieurs responsables du traitement ;
- de créer un cadre réglementaire permettant de tester des traitements policiers à partir de données opérationnelles.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie les responsables politiques de tenir compte des suggestions formulées dans le présent rapport.

Ainsi approuvé par l'Organe de contrôle de l'information policière le 31 octobre 2025.

Copie :

- au chef de corps de la ZP Ninove ;
- au directeur coordonnateur de l'arrondissement de Flandre orientale ;
- au ministre de l'Intérieur ;
- au ministre de la Justice ;
- au commissaire général ;
- au président de la Commission Permanente de la Police Locale.

[57] ISO 270001 A.12.1.4.

[58] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JOUE L* 12 juillet 2024. Plus couramment désigné sous sa dénomination en anglais, à savoir *Artificial Intelligence Act* (*AI Act* ou *AIA*).

Pour l'Organe de contrôle,

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

Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière