RAPPORT DE VISITE ET DE SURVEILLANCE

SYNTHÈSE

VERSION PUBLIQUE[1]

Référence du COC : DIO19005

OBJET : RAPPORT INTERMÉDIAIRE AVEC MESURE CORRECTRICE CONCERNANT LA VISITE MENÉE AUPRÈS DE LA POLICE FÉDÉRALE DE L'AÉROPORT DE ZAVENTEM PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE ET PORTANT SUR L'UTILISATION DE LA RECONNAISSANCE FACIALE À L'AÉROPORT NATIONAL DE ZAVENTEM

[1] La version publique d'un rapport de l'Organe de contrôle ne comporte pas ou pas nécessairement tous les éléments figurant dans le rapport de base adressé aux destinataires. Certains éléments ou passages ont été omis ou anonymisés. Il peut y avoir diverses raisons à cela, qui peuvent être de nature légale ou être dictées par des motifs d'opportunité : la volonté de ne pas divulguer des techniques ou tactiques policières, le secret de l'enquête, le secret professionnel, le fait qu'un manquement a été résolu dans l'intervalle, etc.

1. COMPÉTENCES DE L'ORGANE DE CONTRÔLE

1. La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD) a réformé l'Organe de contrôle de l'information policière (« Organe de contrôle » ou « COC ») en une autorité de contrôle à part entière. L'article 71, §1er et les chapitres II et III de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/13 inclus de la loi du 5 août 1992 sur la fonction de police (LFP), relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de l'intervention policière.

L'Organe de contrôle est compétent pour les services de police[2], pour l'inspection générale de la police fédérale et de la police locale (AIG)[3] et pour l'unité d'information des passagers (BEL-PIU)[4]. La compétence de surveillance de l'Organe de contrôle à l'égard de la police intégrée couvre à la fois les activités de traitement opérationnelles et non opérationnelles[5].

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

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

À travers un contrôle du fonctionnement, l'Organe de contrôle vérifie si le contenu de la BNG et la procédure de traitement des données et informations qui y sont conservées sont conformes aux dispositions des articles 44/1 à 44/11/13 de la LFP et à leurs mesures d'exécution.

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

L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé[7]. Les membres de l'Organe de contrôle et les membres du service disposent à cet égard de compétences d'investigation et peuvent prendre des mesures dites « correctrices »[8].

Un recours juridictionnel peut être introduit dans les 30 jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire[9].

2. OBJET DE LA VISITE ET MÉTHODOLOGIE

[2] Tels que définis à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (art. 26, 7°, a de la LPD).
[3] Telle que définie à l'article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police (art. 27, 7°, d de la LPD).
[4] Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers (art. 26, 7°, f de la LPD).
[5] Art. 4, §2, troisième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.
[6] MAP signifie « méthodes administratives particulières ».
[7] Art. 240, 4° de la LPD.
[8] Art. 244 et 247 de la LPD.
[9] Art. 248 de la LPD.

2.1. Contexte

2. Le 10 juillet 2019, l'hebdomadaire flamand *Knack* a publié une interview avec le commissaire général de la police fédérale, dans laquelle ce dernier annonçait l'utilisation de la technologie de reconnaissance faciale à l'aéroport de Zaventem et l'existence d'un accord à ce sujet avec l'exploitant de l'aéroport et les syndicats. Comme l'Organe de contrôle n'était pas au courant de l'utilisation de cette technologie, le commissaire général a été invité par courrier du 10 juillet 2019 de transmettre à l'Organe de contrôle les informations requises au sujet du déploiement de cette technologie à l'aéroport national. Par courrier du 18 juillet 2019, le déploiement de la reconnaissance faciale a été exposé dans les grandes lignes. L'Organe de contrôle a ensuite mené le 9 août 2019 une visite auprès de la police fédérale de l'aéroport de Zaventem (ci-après abrégée « LPA »).

2.2. Méthodologie

3. À la lumière du courrier du commissaire général du 18 juillet 2019, le contrôle visait concrètement à se faire une idée de la technologie utilisée et à obtenir des informations au sujet du timing prévu, du fondement légal concret, des finalités du traitement, des données à caractère personnel traitées, des mesures prises en matière de sécurité de l'information, de la durée de conservation des données et des banques de données de photographies utilisées.

3. Résultats de la visite

4. Il convient de préciser au préalable qu'au moment de la visite – et en réalité depuis mars 2017 –, le système ne faisait plus l'objet d'une utilisation à part entière.

5. Il ressort du courrier du commissaire général du 18 juillet 2019 que Brussels Airport Company (BAC) a acheté début 2017 pour la LPA un logiciel en vue de tester un système de reconnaissance faciale. Il s'agit de quatre caméras.

Pour simplifier l'explication, le système fonctionne en deux phases. Lorsque le logiciel est activé sur les images des caméras, il prend ce que l'on appelle des « snapshots ». Le système individualise en permanence les images des caméras, créant ainsi un modèle biométrique des personnes, appelé « snapshot ». Ces « snapshots » sont enregistrés et ensuite comparés aux « listes noires » de création propre. Une correspondance « positive » génère un « hit ».

Les tests ayant révélé une marge d'erreur très importante (faux positifs), il y a été mis un terme en mars 2017. De nombreux problèmes avaient notamment été constatés au niveau de la reconnaissance de la couleur de peau, des lunettes et, dans une moindre mesure, de la pilosité (moustache, barbe, etc.).

L'utilisation de la reconnaissance faciale se trouvait par conséquent encore dans une phase de test.

6. Il a cependant été constaté lors de la visite que le système était toujours en partie actif, en ce sens qu'il prend toujours des « snapshots » de tous les passants se déplaçant dans l'aéroport (données biométriques), mais sans les comparer aux photos des listes (noires).

Le système est donc encore *partiellement* actif : des <u>données biométriques sont encore collectées et conservées</u>, mais sans être comparées aux photos de la (des) liste(s).

7. Pour pouvoir (continuer à) tester la fonctionnalité du système, il est indispensable de conserver les images/« snapshots ». Autrement dit, il n'est pas possible de réaliser des tests si les images ne peuvent pas être conservées durant une certaine période minimale. L'avis de l'Organe de contrôle est sollicité à ce sujet :

1) La LPA peut-elle, dans l'état actuel de la législation, recommencer à tester un système de reconnaissance faciale ?

2) Dans l'affirmative, sous quelles conditions et pendant combien de temps les images peuvent-elles être conservées ?

4. CADRE JURIDIQUE APPLICABLE

8. Avant de poursuivre l'enquête et/ou de rendre un avis, la première question qui se pose est (comme toujours) celle du cadre légal applicable – autrement dit, du fondement légal sur lequel reposent le test d'un système de reconnaissance faciale et l'enregistrement des images individualisées (« snapshots »).

Dans son courrier du 18 juillet 2019, le commissaire général adopte à ce sujet le point de vue suivant : *« Bien que la création d'une banque de données technique dans le cadre de la reconnaissance faciale ne soit pas possible dans l'état actuel de la législation, l'utilisation de technologies intelligentes en temps réel autres que la reconnaissance automatique des numéros d'immatriculation (ANPR) est possible en vertu de l'article 25/3 de la LFP. Le législateur a en effet disposé qu'une caméra utilisée par les services de police, quel que soit son type, peut être équipée d'une technologie intelligente. L'introduction d'une reconnaissance faciale en temps réel est donc à notre avis conforme à la loi. »*.

9. Dans l'état actuel du dossier, l'Organe de contrôle n'est pas entièrement convaincu que la LFP soit d'application. Il est vrai que la définition d'une « caméra intelligente » est prise au sens très large. Selon l'article 25/2, §1er, 3° de la LFP, ce terme désigne *« la caméra qui comprend également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies »*. Dans l'exposé des motifs, les caméras ANPR et les caméras permettant la reconnaissance faciale sont notamment citées comme exemples.[10]

La possibilité de tester un système de reconnaissance faciale soulève en premier lieu des questions quant au champ d'application exact du traitement. Lors de la détermination du cadre juridique correct, il n'est en effet pas possible d'établir d'emblée s'il est déjà question, au niveau de l'environnement de test ou pendant une période de test, du traitement de données à caractère personnel dans le cadre de la recherche et de la poursuite – et donc si la LFP et le titre II de la LPD trouvent application. Or, la réponse à cette question est cruciale pour désigner le fondement légal, le niveau de décision habilité au sein de la police à décider de recourir à la reconnaissance faciale, la nature du support de stockage et la durée de conservation, et le niveau de sécurité de l'information à observer (caractère opérationnel ou non).

En second lieu et à titre subsidiaire, l'Organe de contrôle constate toutefois que la LFP, dans l'hypothèse où elle s'applique, décrit bel et bien *ce* qui relève de la définition d'une caméra intelligente, mais *ne stipule pas* dans quelles *circonstances* ni sous quelles *conditions* l'utilisation de caméras permettant la reconnaissance faciale est autorisée, et encore moins sur quel support les images peuvent/doivent être enregistrées et quelles données doivent au minimum être conservées. Dans l'état actuel de la législation, le législateur a exclusivement voulu réglementer la création d'une banque de données technique pour les images ANPR.[11] Selon toutes les informations recueillies par l'Organe de contrôle, les « snapshots » sont bel et bien conservés (temporairement), ce qui implique – à nouveau dans

[10] Doc. Parl. Chambre 2017-2018, n° 54-2588/001, p. 11.

[11] Voir les articles 44/2, §3 et 44/113sexies à 44/11/3decies inclus de la LFP. Le Ministre de l'Intérieur et le Ministre de la Justice ont déclaré durant les débats parlementaires du 2 mars 2018, en l'occurrence le Ministre Geens : *« À la question de savoir pourquoi le projet de loi ne crée des banques de données techniques que pour les données ANPR et non par exemple pour la reconnaissance faciale, le ministre répond qu'étant donné la masse de données à caractère personnel susceptibles d'être récoltées dans ces banques de données, il paraît nécessaire de soumettre chaque technologie spécifique à un débat parlementaire. Il semble néanmoins prématuré de lancer immédiatement le débat sur la reconnaissance faciale. Les répercussions sur la vie privée sont encore considérables. Les données ANPR permettent de rechercher certains véhicules dans des zones bien précises et aussi, avec un peu de chance, les personnes qui s'y trouvent. La reconnaissance faciale permet, elle, de tracer simultanément des personnes – pour autant qu'elles se déplacent en public – à l'aide des dizaines de milliers de caméras. Il semble évident de renforcer davantage les régimes de contrôle sur ce type d'outils très performants. Selon les services de sécurité, cette technologie est encore loin d'être au point et ils ne pourront pas y avoir recours utilement avant un certain nombre d'années. »* (Doc. Parl., Chambre, DOC 54, n° 2855/003). Le Ministre Jambon a pour sa part déclaré : *« Pour ces caméras, il a été décidé que seules les caméras ANPR seraient autorisées par la loi car leur utilisation est déjà très répandue et dès lors que le but poursuivi n'est pas non plus d'empêcher le progrès technologique. »* (Doc. Parl., Chambre, DOC 54, n° 2855/003). Le texte de la LFP est d'ailleurs clair sur ce point et ne laisse en effet aucune place à des banques de données techniques autres que les banques de données ANPR.

l'hypothèse où la LFP/LPD trouve(nt) application – la création d'une banque de données technique contenant des données biométriques, ce qui n'est pas possible dans l'état actuel de la législation.

5. CONCLUSION PROVISOIRE

10. Il ne relève pas de la tâche de l'Organe de contrôle de se substituer à la police – en l'occurrence le responsable du traitement – lorsqu'il s'agit de trancher les questions et remarques qui précèdent. Si la police souhaite recourir aux nouvelles technologies – une idée à laquelle l'Organe de contrôle n'est évidemment pas opposé –, il relève de sa responsabilité de désigner le fondement juridique applicable et de soumettre à l'Organe de contrôle l'analyse de risques et d'impact indispensable et appropriée à l'égard de la protection de la vie privée et de la protection des données à caractère personnel, accompagnée d'une politique et d'un plan de sécurité adéquats et concrets[12]. Ce n'est qu'alors que l'Organe de contrôle sera en mesure de rendre, si requis, un avis en toute connaissance de cause.

L'Organe de contrôle ne peut en outre pas approuver ni autoriser des activités de traitement projetées.

11. L'Organe de contrôle est par contre habilité à prendre des mesures correctrices lorsque des infractions (potentielles) à la législation en vigueur sont constatées. L'Organe de contrôle peut toutefois, comme indiqué plus haut, évaluer la proposition introduite en fonction de la législation en vigueur et juger si l'activité de traitement projetée ou actuelle remplit les conditions imposées par la législation en vigueur. L'Organe de contrôle n'a pas non plus besoin de rappeler que même un projet pilote ou un environnement de test doit répondre aux exigences de légitimité et de régularité, et donc reposer sur un fondement juridique correct, dont l'évaluation revient en premier lieu au(x) responsable(s) du traitement.

À la lumière des constatations qui précèdent, l'Organe de contrôle n'est actuellement pas en mesure (1) de rendre un avis étayé et (2) doit, vu le manque de clarté et les manquements décrits plus haut, imposer une mesure correctrice temporaire.

6. MESURE CORRECTRICE

Par ces motifs,

L'Organe de contrôle de l'information policière,

Prie, en application de l'article 247, 5° de la LPD, le responsable du traitement ou son préposé (la police fédérale « LPA ») de mettre temporairement un terme à l'utilisation du système de reconnaissance faciale, à savoir le traitement de données biométriques, à compter de la date de prise en connaissance de la présente décision, et d'en donner communication et confirmation à l'Organe de contrôle (info@organedecontrole.be).

Conformément à l'article 248, §2 de la LPD, un recours peut être introduit dans les trente jours contre la décision de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire.

Rapport intermédiaire et mesure correctrice approuvés par l'Organe de contrôle de l'information policière le 16 septembre 2019.

[12] Conformément aux articles 58 et 59 de la LPD.