RAPPORT DE VISITE ET DE SURVEILLANCE

SYNTHÈSE

VERSION PUBLIQUE[1]

Numéro de référence : CON19002

OBJET : RAPPORT DE VISITE MENÉE AUPRÈS D'UNE ZONE DE POLICE DANS LA FLANDRE ORIENTALE PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SA COMPÉTENCE DE SURVEILLANCE ET DE CONTRÔLE

[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.

OBJET ET BUT DE LA VISITE

Le 20 juin 2019, l'Organe de contrôle a mené un contrôle d'envergure auprès d'une zone de police locale de la province de Flandre orientale (ci-après dénommée « ZP FLO »). La visite cadre dans la mise en œuvre du Plan stratégique de l'Organe de contrôle, qui vise à rendre visite à un certain nombre de zones de police par an en vue d'exercer ses compétences de contrôle et de surveillance. Le contrôle réalisé auprès de la ZP FLO était une visite spontanée et ne faisait donc pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) de non-respect, par la zone de police controlée, de la législation et de la réglementation. Il a été opté pour une visite en largeur. Cela signifie que la visite portait sur plusieurs thèmes sans s'appesantir trop en profondeur sur les différents thèmes. Une attention particulière était consacrée à l'application du cadre juridique de la protection des données.

Le contrôle portait sur cinq thèmes:
1) Utilisation de caméras
2) Contrôle de la qualité des données et informations contenues dans la BNG
3) Banques de données particulières
4) Systèmes de contrôle du personnel
5) Sécurité de l'information : organisation, politique et gestion des TIC.

Résultats de l'inspection

La ZP FLO a au fil des années élargi progressivement son réseau de caméras, en recourant notamment à des caméras fixes et mobiles permettant la reconnaissance automatique des plaques d'immatriculation (ANPR). Sur certaines voiries de la commune, les caméras ANPR sont utilisées à des fins de contrôle de trajet. La question se pose donc de savoir si cette forme d'utilisation de caméras est soumise aux dispositions de la Loi sur la Fonction de Police (LFP) relatives aux conditions et circonstances de l'utilisation de caméras. L'Organe de contrôle est d'avis que l'utilisation de caméras ANPR à des fins de contrôle de trajet, qui vise donc spécifiquement le contrôle de la vitesse, relève de l'application de la loi du 16 mars 1968 relative à la police de la circulation routière, de sorte que l'utilisation de caméras à cette fin spécifique échappe au champ d'application de l'utilisation de caméras visée par la LFP. Cette forme d'utilisation de caméras est cependant exclue de l'objet de la visite.

Un constat frappant était que la ZP FLO n'était pas en mesure d'apporter une réponse immédiate à la question de savoir par qui ces caméras ANPR avaient été installées et étaient utilisées. L'enquête a révélé que la ZP FLO n'avait pas été informée conformément aux règles légales de l'installation et de l'utilisation de ces caméras par la commune/ville. L'absence de communication ne dispense cependant pas le chef de corps de son obligation de vérifier de sa propre initiative par qui les caméras sont installées et utilisées, et si la législation applicable est respectée dans ce contexte. La ZP FLO utilise aussi des caméras ANPR non visibles. Dans un tel cas de figure, la caméra est montée dans/sur un véhicule de police banalisé. Cette forme d'utilisation de caméras doit cependant faire l'objet d'une déclaration préalable à l'Organe de contrôle. Au moment de la visite, aucune déclaration n'avait encore été faite de l'utilisation non visible de caméras ANPR. De même, aucune déclaration n'avait encore été faite lors de la clôture du rapport.

Au moment de la visite, l'accès aux images des caméras se faisait sur la base d'un identifiant de service général, ce qui n'est pas conforme aux dispositions légales. Il n'était pas fait usage d'un accès individualisable aux images des caméras ANPR, et il ne pouvait être procédé à aucun contrôle du fichier de journalisation des images des caméras ANPR mobiles, s'agissant pourtant là d'une obligation légale. La ZP FLO ne disposait pas non plus pour l'utilisation des caméras d'une gestion des accès et des utilisateurs (concrètement) élaborée. Ces manquements auraient pu être évités ou résolus si la zone de police avait procédé à une analyse d'impact et de risques ou «AIPD»[2] pour (les différentes formes de) l'utilisation des caméras dans la zone de police. Le même constat vaut pour la création des banques de données techniques locales pour les images des caméras ANPR. Pour ces banques de données également, il n'y a eu ni analyse d'impact et de risques ou «AIPD», ni avis du délégué à la protection

[2] Analyse d'impact relative à la protection des données, en anglais « DPIA » pour « Data Protection Impact Analysis ».

des données (ou Data Protection Officer – DPO). La zone de police ne disposait pas non plus d'un registre de l'utilisation des caméras.

Les images des caméras ANPR peuvent être associées à des registres. Cependant, la liste locale de la ZP FLO ne satisfait pas à toutes les conditions légales. Bien que la liste soit soumise à une autorisation de la hiérarchie, les critères d'évaluation n'ont pas été documentés au préalable, de sorte que la proportionnalité de la liste n'a pas pu être évaluée. L'avis du DPO n'a pas non plus été demandé dans ce contexte.

Lors de la vérification des fichiers de journalisation de la BNG, il s'est avéré que la plupart du temps, le motif de la consultation n'était pas indiqué. Aucune directive (politique) n'a été élaborée et aucun contrôle proactif n'est réalisé. La gestion des profils d'accès est assurée conformément à la Circulaire ministérielle MFO3. Il n'y a pas de monitoring continu des profils et des accès en temps réel en fonction de l'effectif réel du personnel. L'alimentation depuis l'application locale vers le niveau central se fait sur une base journalière et les rejets depuis le niveau central sont traités régulièrement. Le contrôle de qualité des dossiers posait problème dans une moindre mesure. L'Organe de contrôle a constaté qu'aucune banque de données particulière n'avait été reprise dans le registre des traitements.

Les services de police traitent également des données à caractère personnel à des fins non policières. Dans ce cas, ces traitements sont soumis non seulement à la loi relative à la protection des données du 30 juillet 2018 (LPD)[3], mais aussi au RGPD 2016/679[4]. Dans ce contexte, la ZP FLO recourt pour l'enregistrement du temps à un système d'enregistrement des empreintes digitales du personnel. De l'avis de l'Organe de contrôle, ce système n'a pas de fondement légal.

La ZP FLO a désigné un délégué à la protection des données, qui dispose des compétences requises et exerce la fonction à temps plein, mais pour plusieurs zones de police. Du fait du grand nombre de zones de police relevant du domaine de travail du DPO, ce dernier est dans l'impossibilité de mener effectivement et efficacement ses missions à bien. Il a été constaté que le DPO désigné, vu le temps limité consacré, n'est pas fondamentalement impliqué dans la mise en œuvre, la gestion journalière et le suivi de la politique en matière de protection des données et de sécurité de l'information. Par ailleurs, la politique en matière de sécurité de l'information n'a pas encore été adaptée à la législation et à la réglementation actuelles. À cet égard, un certain nombre de directives (e.a. l'utilisation d'Office 365 GPI et du Sharepoint, des e-mails et des appareils d'information et de communication) qui étaient annoncées dans l'ordre de service n'ont pas pu être présentées (même pas à l'état de projet).

Les aspects de la sécurité de l'information et de la protection des données peuvent être portés à l'ordre du jour de la réunion hebdomadaire d'une équipe de gestion (sous la direction du chef de corps). Le coordinateur/interlocuteur local en matière de protection de données prend part à ces réunions, mais le DPO n'y assiste pas systématiquement. L'arrêté d'exécution du 6 décembre 2015 obligeait déjà la zone de police à disposer d'un plan de sécurité de l'information, mais ce plan n'était pas disponible lors de la visite.

Un certain nombre de mesures ont été mises en œuvre pour garantir l'intégrité, la confidentialité et la continuité de l'information et des systèmes d'information. Cependant, ces mesures ne font pas l'objet d'un contrôle structurel. Il n'est pas procédé régulièrement à des contrôles internes et autoévaluations en matière de sécurité des TIC (par exemple en procédant à travers des scans de vulnérabilité périodiques à une détection proactive des lacunes dans la protection des systèmes et logiciels informatiques). Il n'a pas non plus été réalisé d'audits de sécurité externes au cours des dernières années.

Le COC a constaté qu'aucune authentification forte n'est requise pour accéder à ce réseau. Il n'est pas procédé à des contrôles proactifs des fichiers de journalisation; ces contrôles ne sont réalisés que sur

---

[3] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. 5 septembre 2018).

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

demande. Aucune procédure ou action de sensibilisation n'a encore eu lieu sur le thème de la dénonciation des fuites de données. Il n'a pas été défini de plan de continuité formel des TIC au sein du service TIC. Des actions ont néanmoins été entreprises par le service TIC de la zone de police pour garantir la disponibilité des données numériques et des systèmes de traitement de l'information.

Conclusion – recommandations – mesures correctrices

Conclusion

Un nombre minime d'aspects des thèmes contrôlés se révèlent (entièrement) conformes à la législation. Un certain nombre de manquements à l'égard des dispositions légales ont d'autre part été constatés. Pour ce qui est des aspects dominant clairement le thème de la protection des données, il s'avère que la ZP FLO ne dispose pas des connaissances spécifiques requises pour apporter une réponse adéquate dans certaines matières sensibles. En dépit de l'engagement manifeste des membres du personnel désignés à consentir dans ce domaine les efforts nécessaires, il se révèle impossible de consacrer suffisamment de temps, en marge des tâches policières journalières, à des formations spécialisées. Ce constat ne peut pas être entièrement compensé par l'assistance du DPO telle qu'elle peut être fournie concrètement.

Le constat général qui précède reflète l'ampleur des manquements concrets constatés. En particulier dans le domaine du recours à la surveillance par caméra et de l'application du cadre légal du droit à la protection des données, il reste un long chemin à parcourir. Il convient d'appliquer dans ce contexte l'adage «réfléchir avant d'agir». La plupart du temps, les autorités de police font l'acquisition d'un système sans procéder au préalable à une évaluation critique de son utilisation en fonction du cadre légal applicable. Il convient de tenir compte non seulement des intérêts du service de police, mais aussi de divers aspects: les intérêts tant de la police que de la personne concernée (autrement dit le citoyen, qu'il habite ou non sur le territoire de la zone de police), la gravité de l'impact du système sur la vie privée de la personne concernée, et enfin le principe *privacy by design*, combiné à une attention marquée pour la sécurité de l'information.

Bien qu'un certain nombre de directives aient été élaborées à l'échelle du corps sur le thème de la sécurité de l'information, la zone de police ne dispose pas d'un plan général de sécurité et de continuité de l'information reposant sur le risque à partir duquel l'organisation, et en particulier le service TIC, pourrait distiller ses propres mesures. Une telle approche reposant sur le risque permettrait d'évaluer, formaliser et documenter les mesures prises. Le service TIC de la zone de police prévoit une série d'initiatives de sécurisation de l'information et de la communication, mais le contrôle périodique (interne/externe) du bon fonctionnement et de l'exhaustivité de ces initiatives n'est pas exercé de manière structurelle et formelle.

Le DPO doit être davantage impliqué dans le suivi, l'adaptation et la mise en œuvre de la politique de sécurité de l'information et de protection des données. Une approche structurelle et un suivi périodique sont à cet égard indiqués.

Il convient dès lors de formuler une série de recommandations qui doivent contribuer à améliorer l'efficacité et l'effectivité du traitement des données (à caractère personnel) réalisé par la zone de police.

Les manquements constatés à l'égard des dispositions légales contraignent cependant l'Organe de contrôle à prendre des mesures correctrices auxquelles la ZP FLO devra donner suite dans un délai bien défini afin de régulariser la situation.

Recommandations

1) Recommandation
Il est recommandé que le chef de corps crée un registre local de l'utilisation de caméras en attendant la promulgation d'un arrêté d'exécution en la matière.

2) Recommandation
À la lumière du manquement constaté, l'Organe de contrôle insiste pour qu'il soit procédé à l'élaboration d'une politique prévoyant un mécanisme de contrôle périodique et effectif (du monitoring) des éventuelles consultations (il)licites.

3) Recommandation
L'Organe de contrôle insiste pour qu'il soit procédé à l'élaboration d'une politique permettant de mettre en place un mécanisme efficace de monitoring continu des profils et de gestion en temps réel des accès en fonction de l'effectif réel du personnel.

4) Recommandation
Bien que l'Organe de contrôle constate des interventions régulières dans la validation centrale, il est souhaitable de ne pas tolérer une accumulation excessive. Il convient dans ce contexte d'aspirer à limiter le nombre de rejets à moins de 100 lignes.

5) Recommandation
Il est important que le chef de corps élabore des directives contraignantes établissant une distinction claire entre les différents aspects visés en ce qui concerne l'accès à l'environnement virtuel. Il convient notamment de distinguer l'accès à Internet pendant les heures de service (recherches, sites autorisés et interdits) de l'utilisation des réseaux sociaux à des fins privées pendant les heures de service, pour autant que des informations policières puissent être partagées. Un volet distinct ou un document séparé décrira (séparément) l'utilisation des appareils mobiles privés à des fins opérationnelles et l'utilisation d'appareils mobiles professionnels à des fins privées. Il est important que le document décrive clairement ce qui est autorisé ou interdit, dans quelles circonstances et sous quelles conditions il peut être procédé à un contrôle, quelles sont les conséquences lorsque des infractions aux dispositions du document sont constatées et quels sont à cet égard les droits de la personne concernée.

6) Recommandation
Il est recommandé de détailler davantage et de revoir régulièrement les directives du corps et les procédures en matière de sécurité de l'information et de protection des données. Il est important dans ce contexte de communiquer ces directives, de les expliquer et de les répéter régulièrement (à travers des campagnes de sensibilisation). Il est par ailleurs important de fournir, en permanence et par le biais de différents canaux d'information (e-mails/intranet/séances d'information/formations/...), des instructions structurelles et périodiques concernant les différents aspects de la sécurité de l'information.

Il est vivement recommandé de motiver les collaborateurs à utiliser les données à caractère personnel et les systèmes d'information et de communication de manière sûre et correcte, à travers l'élaboration, l'application et la communication de bonnes pratiques en la matière.

7) Recommandation
Le COC insiste sur la nécessité d'adapter l'emploi du temps du DPO de la ZP FLO et de limiter le nombre de zones de police pour lesquelles il endosse le rôle de DPO. Le COC est d'avis que dans les circonstances actuelles, le DPO n'est pas en mesure de disposer de suffisamment de moyens (temps) pour exercer de manière adéquate les tâches d'un DPO pour les nombreuses zones de police pour lesquelles il a été désigné.

8) Recommandation
Il est recommandé d'inclure dans le plan de sécurité de l'information les points d'action suivants:

- Actualisation et élaboration plus détaillée de la politique en matière de sécurité de l'information et de protection des données. Cette politique doit être réévaluée régulièrement par le management de manière à ce qu'elle reste pertinente au regard de la réalité.
- Les mesures de maturité et les analyses de risques et de vulnérabilité sont des piliers importants de la politique de sécurité et contribuent à une sécurité de l'information optimale basée sur le risque. Le temps consacré par le DPO à l'exercice de ses tâches constitue également un aspect de cette gestion des risques.

Il est pour ce faire nécessaire de mettre en place des procédures formelles de concertation et de communication avec toutes les parties impliquées, de manière à ce que le DPO soit davantage impliqué dans les activités de l'organisation et dispose à tout moment des informations requises pour mener à bien la mission qui lui a été confiée.

9) Recommandation
L'Organe de contrôle insiste auprès de la zone de police pour autoriser uniquement l'utilisation de comptes d'utilisateur nominatifs/individuels dans le cadre de la gestion opérationnelle.

L'utilisation d'un compte d'utilisateur générique pour l'administration du système doit être limitée le plus possible et n'est autorisée que si elle répond à une exigence technique. Les utilisateurs disposant de droits d'accès étendus, comme les administrateurs de systèmes et d'applications (les «utilisateurs privilégiés»), doivent également exercer leurs tâches journalières dans les systèmes au moyen d'un compte d'utilisateur nominatif. Avec des comptes génériques partagés, il existe un risque qu'il ne soit pas possible de déterminer qui est responsable d'un abus constaté. De plus, un utilisateur privilégié malveillant est en principe en mesure, grâce à ses droits d'accès étendus, d'effacer les traces de ses activités en adaptant par exemple les fichiers de journalisation du système, ou en les supprimant entièrement.

10) Recommandation
La ZP FLO est encouragée à renforcer la surveillance et les contrôles afin de pouvoir disposer d'un aperçu correct et actuel du fonctionnement et de l'efficacité de la sécurité intégrale de l'information. Cela implique notamment :

- le contrôle du respect des obligations légales, réglementaires et contractuelles ainsi que des lignes politiques propres en matière de sécurité de l'information, et plus particulièrement dans le cadre du traitement de données à caractère personnel ;
- le contrôle régulier de la conformité des systèmes d'information aux normes prévues pour la mise en œuvre de la sécurité et l'évaluation de la conformité technique, notamment à travers la réalisation de scans de vulnérabilité, de tests d'intrusion et d'audits/inspections de sécurité ;
- un audit périodique par une tierce partie indépendante, s'agissant là d'un contrôle se dotant d'une incontestable plus-value.

11) Recommandation
Il est indiqué de prévoir des mesures de sécurité additionnelles pour l'utilisation autorisée des supports de données mobiles (clés USB), comme le recours au chiffrement et l'élaboration et la communication régulière d'instructions en vue d'une utilisation sûre des supports de données mobiles.

12) Recommandation
Le COC insiste pour qu'une solution structurelle soit mise en place dans les meilleurs délais pour le monitoring du réseau local (admin/Wi-Fi), et pour qu'une authentification forte (avec des identifiants personnels) soit prévue pour l'accès au réseau sans fil.

13) Recommandation
La zone de police doit élaborer et communiquer une procédure pour la dénonciation des fuites de données. Une sensibilisation régulière sur le thème des incidents en matière de sécurité de l'information, et en particulier des fuites de données, est vivement recommandée.

14) Recommandation
Les profils d'utilisateur pour l'accès aux applications et systèmes d'information et de communication doivent également être tenus à jour conformément à la recommandation formulée pour la BNG.

15) Recommandation
Il est recommandé d'établir un plan d'urgence pour les TIC (DRP ou «Disaster Recovery Plan») ainsi qu'un plan de continuité pour tous les processus critiques et systèmes d'information essentiels de l'organisation, et de tester leur mise en œuvre sur une base périodique. Un DRP pour les TIC va bien plus loin que la seule prévision d'une copie de sauvegarde (back-up). Il doit préparer l'organisation à toutes les calamités possibles susceptibles d'affecter les systèmes d'information et de communication.

Mesures correctrices imposées par le COC

Vu les constatations et recommandations qui précèdent,

Vu l'article 221, §1er et l'article 247, 4°, 5° et 6° de la LPD,

Ordonne à la ZP FLO :

a) de mettre l'accès aux images des caméras en conformité avec l'article 25/7, §1er, troisième alinéa de la LFP, de manière à ce que le motif des consultations soit enregistré. La preuve de cette mise en conformité sera présentée à l'Organe de contrôle dans les six mois à compter de la date de prise en connaissance[5] de cette mesure correctrice ;

b) de déclarer, dans les 15 jours à compter de la prise en connaissance du présent rapport, l'utilisation non visible de caméras ;

c) de déclarer les banques de données particulières soit en REGPOL, soit dans un registre des traitements propre, et d'en faire parvenir la confirmation et l'aperçu à l'Organe de contrôle dans un délai de 2 mois à compter de la prise en connaissance de cette mesure correctrice de l'Organe de contrôle ;

d) de confirmer que dans un délai de trois mois à compter de la prise en connaissance de cette mesure correctrice de l'Organe de contrôle, il sera mis un terme à l'utilisation du contrôle d'accès biométrique, et qu'il ne sera donc plus recouru qu'à un système alternatif une fois ce délai expiré ;

e) de créer un registre des traitements. Ce registre sera mis à la disposition de l'Organe de contrôle dans les 2 mois à compter de la prise en connaissance du présent rapport ;

f) d'établir un plan de sécurité de l'information. Le plan de sécurité de l'information sera mis à la disposition de l'Organe de contrôle dans les six mois à compter de la prise en connaissance du présent rapport ;

Dit pour droit que la date d'entrée en vigueur des mesures correctrices et la date de prise en connaissance desdites mesures telles que visées aux points a) à f) inclus doivent être comprises comme étant la date de la transmission du présent rapport de l'Organe de contrôle augmentée de deux jours (voir aussi la note de bas de page).

Ainsi décidé par l'Organe de contrôle de l'information policière le 7 janvier 2020.

* * * * * * * * *

[5] Le COC prend comme date de prise en connaissance la date de l'expédition du rapport augmentée de deux jours ouvrables (s'il s'agit d'un samedi, d'un dimanche ou d'un jour férié, la date de prise en connaissance est reportée au premier jour ouvrable suivant).