RAPPORT DE VISITE ET DE SURVEILLANCE

SYNTHÈSE

VERSION PUBLIQUE

Numéro de référence : CON19003

OBJET : RAPPORT DE LA VISITE MENÉE AUPRÈS D'UNE ZONE DE POLICE DANS LA PROVINCE DE NAMUR PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SA COMPÉTENCE DE SURVEILLANCE ET DE CONTRÔLE[1]

[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 26 juin 2019, l'Organe de contrôle (COC) a mené une visite d'envergure auprès d'une zone de police locale de la province de Namur (ci-après dénommée «ZP PN»). Cette 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 PN 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 visitée, de la législation et de la réglementation. Il a été opté pour une visite globale. 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.

L'inspection portait sur cinq thèmes:

1) Les mesures visant la sécurité de l'information en général.
2) L'utilisation de caméras.
3) L'accès, l'alimentation et la qualité des données et informations.
4) Les banques de données particulières.
5) La sécurité et la politique en matière ICT.

Résultats de la visite

A travers les réponses obtenues au questionnaire transmis par le COC préalablement à notre visite et aux observations réalisées au sein de la ZP PN, il a été constaté que cette zone disposait d'une bonne connaissance des différentes législations et directives policières en matière de traitement des données à caractère personnel et de gestion de l'information.

Il a été constaté que la direction de la ZP PN fait preuve d'une réelle volonté de mettre en œuvre une politique active en matière de protection des données et ce à travers différentes actions. La ZP PN a mis en place dès début 2018 un DPO et lui a permis de suivre différentes formations spécifiques à sa fonction.

Le DPO de la ZP est fortement 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

Afin de déterminer un état des lieux en matière de protection des données, le DPO a réalisé dans le courant de l'année 2018 un audit interne. Les résultats ont été communiqué à la direction de la ZP et afin qu'il puisse remédier aux différentes carences constatées.

Nous avons pu remarquer lors de notre visite que de nombreuses initiatives avaient été entreprises suite à cette audit, à l'exception de quelques points qui devaient encore être réalisés. La ZP a également mis en place différents groupes de travail au sein de ces différents piliers afin de transposer les nouvelles directives en matière de protection des données. A travers différents exemples concrets nous avons pu remarquer que la ZP PN, était à l'origine de différentes initiatives et de bonnes pratiques en matière d'application du GDPR partagées au niveau de l'arrondissement (province) de Namur.

A l'heure actuelle, il n'existe plus au sein de la ZP PN de véritable plan de sécurité de l'information au sens ICT, celui-ci a été inclus dans le plan « protection des données ».

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 ICT (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.

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, notamment dans la réalisation correcte et complète du triptyque (prendre les empreintes digitales, prendre des photos et faire la description individuelle).

En ce qui concerne les banques de données particulières, l'Organe de contrôle a constaté que ces dernières (152) sont correctement encodées dans le registre REGPOL. L'accessibilité à ces différentes banques de données est basée sur le principe du «besoin d'en connaître». Ces différentes banques de données sont accessibles via différents software qui ne garantissent pas toujours une traçabilité et un contrôle des accès suffisant.

La ZP PN dispose d'un réseau de 168 caméras visibles, une analyse d'impact et de risques a été réalisée et transmise au COC en mai 2019. Ces différentes caméras ont également été enregistrées et répertoriées dans l'application informatique « Camélia ».

La gestion et le traitement des images issus de ces caméras sont réalisés à l'aide d'un logiciel spécifique installé sur un réseau séparé. L'accessibilité à ce logiciel n'est possible que sur un nombre limité d'ordinateurs, sur base d'un identifiant personnel et selon le profil attribué. L'accessibilité aux images en live est possible sur l'ensemble des ordinateurs disposant du logiciel spécifique et ce après s'être loggé. Les demandes d'images archivées, s'effectuent à l'aide d'un formulaire généré dans l'ISLP[2]dans lequel le demandeur doit s'identifier et détailler l'objet de sa demande. Les moyens mis en place permettent une traçabilité des demandes mais aucun contrôle proactif n'est actuellement mis en place par la ZP.

Dans le courant de l'année 2018, la ZP a décidé de se doter de Bodycam (Caméra piéton). A cet effet une phase test a été réalisée et à l'issue de celle-ci, la ZP a décidé d'équiper son personnel de cette technologie. Une analyse d'impact et de risques au niveau de la protection de la vie privée a été réalisée et validée en date du 23 novembre 2018 et transmise au COC. Dans un soucis de transparence et de communication externe, la ZP PN a informé la population locale à travers le bulletin communal de l'utilisation prochaine de bodycam par les membres du personnel de la ZP PN. Une note de service intitulée *'Directives opérationnelles relatives à l'usage de bodycams (« Caméras piétons »)'* a été rédigée et diffusée en date du 18 avril 2019 à l'ensemble du personnel de la ZP. Lors de notre visite, le personnel de la ZP PN n'était pas encore équipé de cette technologie, ce qui implique que le COC n'a pas pu vérifier la mise en place et l'usage dans la pratique quotidienne.

Au moment de la visite la ZP PN ne disposait pas de caméra dotée de la technologie ANPR, de ce fait nous n'avons pu vérifier l'utilisation de cette technologie. La ZP PN envisage dans un avenir proche de recourir à la technologie ANPR, dans ce cadre une analyse d'impact et de risques a été réalisée en date du 03 juin 2019.

Au moment de notre visite, la ZP PN n'utilisait pas de caméras non-visibles (cachées).

[2] Integrated System for the Local Police.

Lors de notre visite, il a été constaté que certains membres du personnel de la ZP avaient tendance à utiliser des appareils personnels et des messageries privées du type *WhatApps*. La ZP PN est bien consciente de cette pratique mais n'a mis en place aucune politique par rapport à cette problématique sachant que la mise en place dans le courant du second semestre 2019 de l'application «*Focus I-police*» fera disparaître cette pratique.

Conclusion – recommandations – mesures correctrices

Conclusion

La visite du COC a permis de constater que la ZP PN avait depuis 2018 développé différents projets, actions et de bonnes pratiques en matière de protection des données et de sécurité de l'information.

La ZP PN est d'ailleurs à l'origine de différentes initiatives en matière de protection des données au niveau de l'arrondissement de Namur et ce afin de partager les expériences et les connaissances en la matière.

Le constat général qui précède reflète la volonté de la ZP PN de s'inscrire dans une politique active en matière de sécurité de l'information. Au cours de notre visite nous avons pu constater que la ZP dispose des connaissances spécifiques requises pour apporter une réponse adéquate à l'ensemble des problématiques liées aux différentes thématiques touchant à la protection des données personnelles et à la sécurité de l'information en général.

La visite a également permis de constater la volonté de la ZP PN de s'inscrire dans un processus de modernisation des outils policiers et de tendre vers le développement d'une digitalisation plus accrue du travail policier. En effet la ZP s'inscrit dans de nombreux projets en qualité de zone pilote, comme notamment l'implantation de l'application *I-Police Focus*, l'utilisation de bodycam, l'utilisation de caméras dotées de la technologie ANPR. Dans ces deux derniers cas la ZP a privilégié une démarche de réflexion en effectuant tout d'abord une analyse d'impact et des risques au niveau de la protection de la vie privée et ensuite une phase test afin de pouvoir essayer différents types de matériels. Mais également en faisant du benchmarking auprès d'unités utilisant déjà cette technologie.

Néanmoins nous avons tout de même pu constater au cours de la visite que la ZP PN devait continuer de s'investir dans certains domaines où quelques manquements ont été relevés et ce afin de tendre vers l'excellence dans la politique qu'elle mène en matière de protection des données à caractère personnel et de la sécurité de l'information.

Bien qu'un certain nombre de directives aient été élaborées ou sont en cours d'élaboration à l'échelle du corps sur la thématique de l'accès aux différentes banques de données depuis notre visite, la ZP PN doit rester attentive à cette problématique.

La ZP PN doit également poursuivre ses initiatives en matière de sécurité physique de ces locaux et continuer d'investir dans ce domaine.

Une attention particulière est également recommandée en matière de sécurité ICT, la zone de police ne dispose pas d'un plan général de sécurité ICT. Un tel plan permettrait d'identifier et d'évaluer les risques et de déterminer les mesures de protection ad-hoc. Une telle approche reposant sur le risque permettrait d'évaluer, formaliser et documenter les mesures prises.

Suite à notre visite et à nos remarques la zone de police nous a signalé qu'elle allait mettre en place durant l'année 2020 une série d'initiatives de sécurisation de l'information, mais également des tests périodiques BRP/BCM (*Disaster Recovry*/ *Business Continuity*).

Il convient dès lors de formuler une série de recommandations d'accompagnement qui doivent contribuer à améliorer l'efficacité et l'efficience de la ZP PN en matière de gestion et de traitement des données à caractère personnel en particulier et de l'information policière en général .

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

Recommandations

1) Recommandation

À la lumière du manquement constaté, l'Organe de contrôle insiste pour qu'il soit procédé à l'élaboration d'une politique en matière d' accès illégitime aux banques de données. Cette politique se traduira par un mécanisme de contrôle périodique et effectif (du monitoring) des éventuelles consultations (il)licites et par l'élaboration d'une directive afin de rappeler les règles et les obligations du personnel en matière de consultation des banques de données, notamment la traçabilité des données consultées.

2) Recommandation

Il est recommandé de détailler davantage et de revoir régulièrement les directives du corps et les procédures en matière d'alimentation de la BNG. 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 liés à l'alimentation de la BNG.

Il est recommandé d'améliorer la procédure de contrôle de la qualité de l'encodage de la BNG, mais également de renforcer le contrôle d'encodage aux différents niveaux hiérarchiques.

3) Recommandation

Il est recommandé à la ZP PN de s'assurer qu' à travers la mise en place de l'application «Focus», l'utilisation d'appareil ou de messagerie privée sera inexistante. Bien qu'une directive encadrera l'utilisation des appareils mis à disposition par la ZP PN, nous recommandons que l'encadrement soit attentif à ce point.

4) 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.

5) 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.

6) 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.

7) Recommandation

Il est recommandé d'établir un plan d'urgence pour les ICT (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 ICT 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.

Mesure(s) correctrice(s) imposée(s) 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 PZ PN :

a) d'établir un plan de sécurité de l'information ICT. 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;
b) de transmettre au COC, les résultats des tests *BRP/BCM* qui seront effectués, ainsi que les mesures correctrices qui seront mise en place ;
c) de mener au minimum 4 fois par an des contrôles proactifs aléatoires en matière de consultations illégitimes des banques de données et de tenir informé le COC des résultats.

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 c) inclus doivent être comprises comme étant la date de la transmission du présent rapport de l'Organe de contrôle augmentée de deux jours.

Ainsi décidé par l'Organe de contrôle de l'information policière le 27 janvier 2020.

* * * * * * * * *