TABLE DES MATIÈRES

Enquête de contrôle sur les moyens mis en œuvre par la police intégrée pour limiter les risques liés à l'accès à l'information policière, singulièrement celle relative au domaine opérationnel et/ou dit(e) sensible

1 CONTEXTE ET RÉSUMÉ DE L'ENQUÊTE

Le Comité permanent P a opté pour la réalisation d'un suivi des recommandations formulées dans l'enquête de contrôle sur les moyens mis en œuvre par la police intégrée pour limiter les risques liés à l'accès à l'information policière, singulièrement celle relative au domaine opérationnel et/ou dit(e) sensible.

L'objectif de l'enquête de base visait à établir un état des lieux de la sécurité de l'accès à l'information policière dans les services de police. Dans cette enquête, les recommandations suivantes avaient été formulées :

- étant donné la période de limitation budgétaire, ne pas céder à la « tentation » de réduire à outrance les investissements en matière de sécurité (de l'information ou autres) ;
- désigner au plus vite les conseillers en sécurité et en protection de la vie privée et faciliter l'exécution de leurs missions ;
- ajouter rapidement au programme des académies une formation spécifique pour les conseillers en sécurité et en protection de la vie privée dépassant le cadre de la simple information et portant sur les aspects de management, informatiques et légaux relatifs à cette fonction ;
- à moyen terme, compte tenu de l'évolution rapide de l'environnement (technologies, menaces, pratiques,…), la fonction devra être soutenue par des recyclages réguliers, que doivent prévoir les futurs plans de formation ;
- respecter l'indépendance qui doit être conférée à ce rôle de conseiller en sécurité et en protection de la vie privée et éviter de cumuler ce rôle avec certaines autres fonctions, en particulier celle de gestionnaire-système.

Pour effectuer ce suivi, des entretiens et recueils d'information avec les responsables du Commissariat général - CG/Information Security & Privacy Office (SIVP) ont été effectués fin de l'année 2016. Il a été tenu compte du cadre normatif élaboré au niveau européen.

2 CONSTATATIONS

2.1 DÉSIGNATION DES CONSEILLERS DANS LES CORPS DE POLICE

L'arrêté royal relatif à la désignation des conseillers en sécurité et en protection de la vie privée a été publié le 6 décembre 2015. La police fédérale a établi la liste des conseillers désignés en son sein et allait communiquer incessamment les noms (~50 personnes) à l'organe de contrôle (COC) et à la commission de la protection de la vie privée (CPVP).

Les polices locales doivent également communiquer le nom des personnes désignées aux deux instances. Le SIVP, service fédéral, n'a pas de vue sur le niveau local mais la Commission Permanente de la Police Locale (CPPL) a précisé que, dans la plupart des cas, les zones de police ont désigné leur conseiller[1]. Il est rappelé que vu l'autonomie de gestion liée à la structure policière à deux niveaux, il n'est pas prévu de désigner un conseiller pour l'ensemble de la police intégrée.

Au niveau fédéral, le profil de fonction du conseiller en sécurité et en protection de la vie privée a été repris dans le T03 (tableau organique dressé suite à l'optimalisation de la police fédérale) au niveau déconcentré.

---

[1] D'autre part, cette fonction peut être exercée au profit de plusieurs zones.

En 2012, l'Union européenne a décidé de réformer la protection des données à caractère personnel et de mettre en place un nouveau règlement. En avril 2016, deux textes ont été publiés : le RGPD (Règlement Général sur la Protection des données, également appelé GDPR pour General data protection regulation)[2] pour tous secteurs (privés et publics) ainsi qu'une directive pour le domaine de la police et la justice[3]. Ces deux textes devront être intégrés en droit belge pour mai 2018 au plus tard et modifieront en profondeur notamment la loi sur la protection de la vie privée ainsi que la loi sur la fonction de police.

2.2 FORMATIONS PROPOSÉES DANS LES ACADÉMIES DE POLICE

En ce qui concerne les formations, deux domaines sont à distinguer : privacy et sécurité. Les formations pour les conseillers en matière de sécurité ne sont pas encore effectives. Plusieurs partenariats sont prévus avec d'autres services publics mais n'ont pas encore pu se mettre en place pour diverses raisons. En matière de privacy, il n'y a pas de formation dispensée structurellement.

Une formation modulaire en protection des données à caractère personnel est en cours d'élaboration. Deux modules de cours ont déjà été donnés fin 2015-début 2016. Ils portaient sur : « protection des données à caractère personnel : concepts de base et principes généraux » et « protection des données à caractère personnel : spécificités des données opérationnelles ». Cette formation est à destination principalement des membres du personnel de la police fédérale mais les membres de la police locale peuvent y participer.

D'autres modules thématiques devraient suivre : spécificité des données opérationnelles, application de la directive interne[4] « ICT-privacy » portant sur les règles en matière de données relatives aux badges d'accès, numéros de téléphones, de GSM, utilisation et contrôle des réseaux ICT au sens large, etc.

Les formations sont développées également avec l'aide d'acteurs comme DGR-DRI (Direction de l'information policière et ICT) et Interpol. Mais il faut signaler que les connaissances en la matière sont concentrées auprès de quelques personnes.

2.3 MISE EN PLACE DE LA PLATEFORME DE LA SÉCURITÉ ET DE LA PROTECTION DES DONNÉES

À ce stade, la plateforme n'existe pas encore. Bien que l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences du commissariat général spécifie à l'article 2.1°.e) : *« en concertation avec la Commission permanente de la police locale, la détermination de normes et d'une approche standardisée en matière de sécurité de l'information et de protection de la vie privée applicables à la police fédérale ou à l 'ensemble de la police intégrée »,* aucune étape n'avait été entreprise par le SIVP au moment de notre visite pour en coordonner la mise en place en raison du manque de capacité de ce service. Entre-temps, des démarches ont été accomplies avec la CPPL en vue de créer cette plateforme.

La plate-forme de la sécurité et de la protection des données devrait servir également de lieu de formation.

2.4 DÉVELOPPEMENT DE LA POLITIQUE DE SÉCURISATION ET DE PROTECTION DE LA VIE PRIVÉE AU SEIN DES CORPS DE POLICE

Une complexité inhérente au travail de police est la nécessité de gérer des données de différentes natures, dont les données opérationnelles ne constituent qu'une partie.

Comme évoqué précédemment, l'Union européenne a réformé le cadre légal visant la protection des données et de mettre en place un nouveau règlement de protection. Certaines dispositions du RGPD ainsi que de la directive (UE) 2016/680[5] destinée aux secteurs de la police et de la justice pénale devront être

---

2 Ce règlement portant le numéro (UE) 2016/679 est entré en vigueur le 24 mai 2016, mais à compter de cette date une période de transition de 2 ans est prévue. La Commission vie privée, les entreprises et les organisations ont jusqu'au 25 mai 2018 pour se plier aux exigences du RGPD (source : https://www.privacycommission.be).

3 Directive (UE) 2016/680.

4 Cette directive est en phase finale de développement. Elle sera applicable dès diffusion.

5 Directive « police justice » : directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

précisées par le droit belge pour mai 2018 au plus tard. Par ailleurs, les autres dispositions belges portant sur la CPVP et les mesures concrètes devront être adaptées pour être conformes au RGPD.

La police fédérale par l'intermédiaire du SIVP participe aux travaux européens ainsi qu'aux réunions de coordination chapeautées par le SPF Justice avec pour objectif l'application de ces textes pour 2018.

Le titre complet de la directive « police justice » pourrait laisser entendre qu'elle ne s'applique qu'aux missions de police judiciaire mais elle couvre également les activités de police administrative. Cependant, lorsque les services de police traitent des données à caractère personnel pour d'autres fins, par exemple dans le cadre de la gestion du personnel, le RGPD devrait s'appliquer.

Par rapport à la législation actuelle, le RGPD renforce les droits des personnes concernant leurs données personnelles. Pour ce faire, les rôles et les responsabilités de l'autorité de contrôle[6], du responsable du traitement et du délégué à la protection des données sont sensiblement accrus, ce qui ne peut qu'avoir une influence positive sur la sécurité générale des données, qui fait l'objet de la présente enquête. Le RGPD met également en avant certaines procédures et techniques telles que l'anonymisation, la pseudonymisation et le cryptage.

La directive « police justice » prévoit la possibilité de limiter les droits de la personne concernée d'être informée de l'existence d'un traitement de ses données, d'y avoir accès ainsi que de les rectifier ou les effacer, lorsque l'exercice de ces droits est susceptible par exemple de gêner des enquêtes, de prévenir ou détecter des infractions ou de protéger la sécurité publique. Il est à noter que la directive insiste sur l'importance dans une société démocratique des principes de nécessité, proportionnalité et subsidiarité que doivent respecter ces limitations. D'autre part, cette directive a également pour but de faciliter l'échange transfrontalier d'informations policières.

En ce qui concerne les zones de police, il est probable que certaines soient avancées dans l'établissement de leur politique de sécurité des données et de la vie privée mais, à nouveau, la police fédérale n'a pas de vue sur celle-ci. Il faut réaliser que la « politique » est un concept large, qui pourrait être matérialisé, par exemple, dans un règlement d'ordre intérieur selon ce que décide la zone.

2.5 Synergies avec le Centre pour la cyber sécurité Belgique (CCB) ou d'autres organismes

En matière de sécurité des informations, le CCB élabore, coordonne et veille au respect des normes, standards et directives de sécurité pour les systèmes d'information des services publics. Le CCB travaille au profit de l'ensemble du territoire (privé-public, citoyens,…) et en collaboration avec d'autres services dont les services de police d'après les informations obtenues.

En matière de suivi des cyber-attaques, les menaces sont suivies constamment par la police fédérale en concertation avec le CCB et les autres SPF. Les informations et expériences sont échangées et rediffusées ensuite aux membres de la communauté policière et aux services externes. Toutefois, il n'y a pas encore de structure mise sur pied pour communiquer avec les zones de police.

3 Conclusions

Les mesures à mettre en place en matière de sécurité de l'information et respect de la vie privée, exposées dans l'enquête initiale ne sont pas encore entièrement d'actualité. Il faut constater qu'il s'agit d'une matière spécialisée et en constante mutation, partant du niveau international. L'expertise et la connaissance pour appréhender les concepts et principes et les concrétiser en un cadre normatif se concentrent dans un nombre réduit d'experts ; de plus, la quantité et la nature des données gérées par les services de police sont très importantes.

Parmi les freins évoqués dans la mise en place de ces mesures, un manque de capacité et certaines autres priorités sont cités. Les politiques en matière de sécurité et de vie privée sont de la compétence de chaque corps de police. La police fédérale n'a pas de vue sur les initiatives des zones de la police locale. La structure policière ne prévoyant pas d'organe de coordination en matière de sécurité de l'information et de

6 La directive requiert la mise en place d'au moins une autorité de contrôle indépendante vérifiant le respect de son application.

protection de la vie privée entre les deux niveaux de police, des initiatives devront probablement provenir du niveau local pour la concrétisation de la plateforme ou pour la désignation des futurs acteurs. Il existe bien le comité de coordination de la police intégrée (CCGPI)[7] mais ce comité est avant tout chargé de stratégie policière.

L'enjeu est l'année 2018, qui verra la retranscription en droit belge de directives européennes plus exigeantes en matière de sécurité des données à caractère personnel : le RGPD et la directive (UE) 2016/680.

Les services de police devront donc être prêts à ce moment. Il semble nécessaire que les mesures en développement, comme la formation des conseillers, la plateforme de coordination, la coordination entre les zones de police et entre celles-ci et la police fédérale, soient dorénavant appréciées à l'aune de la transposition en droit belge du RGPD et de la directive « police justice ». Par exemple, la formation des conseillers devrait déjà maintenant tenir compte du rôle et des responsabilités accrus du futur délégué à la protection des données.

En exigeant de tous les acteurs de la police et de la justice une meilleure intégration de la protection des données à caractère personnel dont ils sont dépositaires, ainsi qu'une meilleure conscientisation des risques encourus, ces textes devraient avoir une incidence positive sur l'amélioration de la sécurité des données policières au sens large.

Le Comité P constate que les services de police ont bien intégré la menace extérieure provenant en particulier des organisations criminelles et terroristes. Toutefois, il tient à rappeler l'existence d'une « menace » interne qui peut prendre la forme d'actions mal intentionnées mais aussi (et sans doute bien plus fréquemment) d'erreurs ou de négligences lors de la conservation ou de la transmission de données, et qui doit être impérativement prise en compte lors de la conception des systèmes d'information et de l'établissement des procédures (*cf.* la « privacy by design » prônée par le RGPD).

7 26 MARS 2014 - loi portant mesures d'optimalisation des services de police, insertion article 8ter dans la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.