ANNEXE H.

AVIS DU COMITÉ PERMANENT R SUR UN AVANT-PROJET DE LOI RELATIF À L'UTILISATION DE CAMÉRAS

Dans son courrier du 2 août 2017, le ministre de la Justice a, au nom du Conseil des ministres, demandé l'avis du Comité permanent R sur le 'Chapitre IV de l'avant-projet de loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.

Le Comité permanent R souhaite formuler plusieurs remarques générales et spécifiques.

La nécessité (de certains aspects) du projet ?

Dans le projet d'Exposé des Motifs, il est établi que '*[…] une utilisation directe des caméras dites "policières" en temps réel ou un accès direct aux bases de données policières par les services de renseignement et de sécurité ne sont pas prévus dans la loi*'. Le Comité s'interroge sur ce postulat.

En effet, l'utilisation **en temps réel** de caméras de la police, voire de particuliers (par exemple, des entreprises de gardiennage), est déjà possible actuellement par le biais d'une méthode spécifique ou exceptionnelle, en fonction de la nature du lieu observé. Dans la réglementation actuelle, il n'est précisé nulle part que dans le cadre d'une observation réalisée à l'aide d'un moyen technique, celui-ci doit appartenir au service de renseignement concerné.[1] À cet égard, les articles 83 et 84 du projet sont superflus. En outre, demander des **images déjà enregistrées** ne constitue pas en soi une méthode particulière de renseignement, mais bien une méthode ordinaire, à laquelle s'applique l'article 14 ou 16 L.R&S, en fonction du responsable du traitement (public ou privé). En sa qualité d'organe juridictionnel, le Comité a déjà pris une décision en ce sens.

'Le Comité permanent R a été informé de la décision de procéder à *'de exploitatie van beelden gefilmd door een camera toebehorend, geplaatst en beheerd door een private bewakingsfirma.' ('l'exploitation d'images filmées par une caméra placée et gérée par une société de surveillance privée'* – traduction libre). Il ressort des informations récoltées que le service concerné n'avait pas le moindre contrôle sur l'endroit où la caméra avait été installée ni sur les images et les périodes filmées. Cette caméra était gérée en toute indépendance par une société de surveillance. Le Comité a estimé '*dat het louter ontvangen en bekijken van beeldbanden, gemaakt door een camera die door de beheerder van een camerasysteem ter beschikking worden gesteld, geen observatie uitmaakt in de zin van de Wet van 30 november 1998. Deze methode vormt aldus geen specifieke methode doch slechts een gewone methode.*' (*'que la stricte réception et le strict visionnage de bandes vidéo, enregistrées par une caméra mise à disposition par le gestionnaire d'un système de caméras, ne constituent pas une observation au sens de la Loi du 30 novembre 1998. Il ne s'agit dès lors pas d'une méthode spécifique, mais seulement d'une méthode ordinaire'* – traduction libre).

[1] Ce qui ne signifie pas que les services de renseignement qui procèdent à une observation au moyen d'une caméra appartenant à des tiers, peuvent aussi 'sous-traiter' l'opération à ces tiers. Conformément à la jurisprudence du Comité permanent R, le service de renseignement concerné doit toujours rester 'maître' de la méthode utilisée.

Cela concerne en effet '*het (inwinnen van) inlichtingen noodzakelijk voor de uitoefening van hun opdrachten, met inbegrip van persoonsgegevens, […] bij elke persoon of organisatie die behoort tot de privé-sector*' (*'le recueil d'informations nécessaires à l'exercice de leurs missions, y compris des données à caractère personnel, auprès de toute personne ou de tout organisme relevant du secteur privé'* – traduction libre), tel que visé à l'article 16 L.R&S et/ou le recueil de renseignements par le biais de sources humaines tel que visé à l'article 18 L.R&S. Le Comité s'est néanmoins empressé d'ajouter que cela ne signifiait pas nécessairement que l'utilisation de cette méthode ne pourrait pas être problématique au regard, par exemple, des exigences de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en général, et de la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, en particulier. Cette problématique ne relève toutefois pas de la compétence du Comité en tant qu'organe juridictionnel.' (COMITÉ PERMANENT R, *Rapport d'activités 2010*, 69).

En ce qui concerne la demande d'images déjà enregistrées ou d'autres informations qui sont détenues par les services de police, le Comité souligne en outre que l'article 14 alinéa 4 L.R&S prévoit également la possibilité d'accéder directement aux banques de données du secteur public (qui comprend les services de police), dans les conditions fixées par le Roi. Cette possibilité existe donc déjà, pour autant qu'un Arrêté royal en précise les conditions.

Ce qui n'est pas encore clairement réglé, c'est la **corrélation permanente** des banques de données d'un service de renseignement, des listes ou des critères d'évaluation préétabli par celui-ci avec des données (uniquement provisoirement) ANPR. Une telle méthode est potentiellement très intrusive et peut donner lieu à un suivi étendu de personnes ou de groupes de personnes. Par conséquent, le contrôle exercé sur ce genre de recueil de renseignements doit être proportionnel (voir *infra*), surtout si, à l'avenir, d'autres systèmes intelligents venaient à être utilisés (par exemple, la reconnaissance faciale ou la reconnaissance de certains comportements). Eu égard au caractère potentiellement intrusif de cette méthode, la réglementation légale doit être suffisamment précise. Ainsi, il convient de clarifier la notion de 'corrélation' dans le projet, et de déterminer quelles données les listes peuvent contenir et quels critères d'évaluation sont autorisés ou non.

Complexité du projet

Le Comité tient à souligner que les articles concernés – qui doivent être lus conjointement avec la Loi sur la fonction de police et la Loi caméras – se sont singulièrement complexifiés et sont donc sujets à interprétation. Par ailleurs, l'Exposé des Motifs n'apporte pas toujours la clarté requise. L'étendue exacte de ces dispositions, dont l'application peut se révéler très intrusive, ne semble pas répondre aux exigences de (l'article 8 de) la CEDH.
En raison notamment des nombreuses modifications substantielles apportées récemment à la L.R&S, les personnes sur le terrain risquent de perdre la vue d'ensemble sur le choix du moyen de collecte et du régime à appliquer : une méthode ordinaire que l'agent de renseignement peut utiliser en toute autonomie ou pour laquelle l'autorisation d'un officier de renseignement ou du dirigeant du service est requise, une méthode ordinaire assortie d'une modalité de contrôle supplémentaire par le Comité, une méthode spécifique ou une méthode exceptionnelle.

Dans un précédent avis, le Comité a déjà souligné le fait que la logique interne qui sous-tend les méthodes ordinaires, spécifiques et exceptionnelles (variant en fonction du degré d'intrusion) risque de disparaître. Le Comité a attiré l'attention, entre autres, sur le règlement PNR, qui est double : la demande de données des vols internationaux constitue une méthode ordinaire et la demande des déplacements, par exemple en train à grande vitesse, constitue une méthode spécifique. La réglementation élaborée dans cet avant-projet renforce encore cette complexité.

Le projet d'article 16/4 § 1er L.R&S

L'article 16/4 § 1er L.R&S prévoit une réglementation spécifique pour l'accès direct aux '*informations et données à caractère personnel qui sont collectées au moyen de caméras dont l'utilisation par les services de polices est autorisé[e]*'.

À cet égard, la possibilité d'**accéder directement** concerne *toutes* les banques de données policières, c'est-à-dire la BNG, les banques de données de base, les banques de données particulières et les nouvelles banques de données techniques (en effet, il est fait référence à l'art. 44/2 de la Loi sur la fonction de police) et concerne également *toutes* les images provenant de caméra (pas uniquement ANPR). Cependant, l'accès n'est autorisé que pour les images provenant de caméras. Le Comité s'interroge sur la manière dont cette possibilité peut être opérationnalisée. Les services de renseignement pourront-ils ou devront-ils effectuer des recherches dans tous les banques de données policières pour (seulement) visionner/télécharger des images provenant de caméras ?

Comme déjà indiqué ci-avant, le Comité ne comprend pas non plus pourquoi une réglementation particulière doit être élaborée pour les données policières qui sont recueillies via des caméras, et pourquoi on ne peut pas, en la matière, prendre appui sur l'article 14 L.R&S.

Il ressort de l'Exposé des Motifs que le projet d'article 16/4 § 1er L.R&S permettrait également un ***live feed*** des images policières. Le Comité est d'avis que cette possibilité, en fonction des circonstances concrètes (par exemple, l'utilisation d'une caméra de la police pour contrôler en permanence qui entre dans un immeuble déterminé), doit être synchronisée avec une observation spécifique ou exceptionnelle. À ce moment-là, les règles relatives à l'utilisation des méthodes particulières doivent être appliquées. À défaut, la réglementation actuelle dans ce domaine serait vidée de son contenu, par exemple en ce qui concerne le délai de conservation des données ainsi obtenues par les services de renseignement. À cet égard, le Comité attire l'attention sur les articles 83 et 84 de l'avant-projet, qui permettent l'utilisation de caméras dites 'policières' dans le cadre de méthodes spécifiques et exceptionnelles.

Le projet d'article 16/4 § 2 L.R&S

À la lecture de l'Exposé des Motifs, l'article 16/4 § 2 L.R&S concerne l''***accès a posteriori*** *aux données collectées*'. Le Comité ne voit que peu de différence avec le § 1er, prévoyant également un accès à des données enregistrées par des caméras.

Néanmoins, aucun arrêté d'exécution particulier n'est requis dans le § 2, et les données ne semblent pas pouvoir être protégées lorsqu'elles s'inscrivent dans une enquête pénale en cours (voir également *infra*). Un autre régime d'accès et de contrôle est également prévu. De plus, la

consultation doit être 'ciblée'. Cette exigence laisse naturellement une grande marge d'interprétation : le téléchargement de toutes les images de caméras d'une région donnée pendant une période donnée est-il 'ciblé' ?

Le Comité constate que pour accéder à des données qui ont été enregistrées plus d'un mois auparavant, le dirigeant du service doit donner son autorisation, alors que c'est le procureur du Roi qui la donne aux services de police dans le cadre d'une enquête pénale. En outre, le dirigeant du service peut déléguer cette mission, si bien que ce même officier de renseignement peut encore prendre sa décision jusqu'au moment de l'accès.

Le Comité estime que le contrôle prévu n'est pas proportionnel au caractère potentiellement intrusif de la nouvelle méthode :

- Les décisions des officiers de renseignement ne sont pas portées à la connaissance du Comité.
- Aucun délai n'a été fixé pour signifier les décisions du dirigeant du service au Comité.
- Si, dans le cadre d'une enquête de renseignement, plusieurs consultations ciblées doivent être effectuées (ce sera généralement le cas), la liste est transmise chaque mois. Il est dès lors impossible qu'un contrôle soit effectué à temps.
- Entre autres en raison des nouvelles tâches qui lui ont été confiées récemment, le Comité ne dispose pas d'effectifs, de moyens budgétaires ni de moyens techniques suffisants pour être réellement et effectivement en mesure d'assurer cette mission de contrôle supplémentaire.

Le Comité tient à souligner le fait que la destruction de données dans un contexte de renseignement a souvent plus une valeur symbolique et ne change pas grand-chose pour le fonctionnement des services de renseignement. Les données détruites, le cas échéant, ne doivent en effet pas servir dans l'une ou l'autre procédure, par exemple comme preuves.

Le projet d'article 16/4 § 4 L.R&S

Le projet d'article 16/4 § 4 L.R&S introduit une nouvelle possibilité de grande portée pour les services de renseignement. Il s'agit d'une forme de ***datamining*** (exploration de données), par lequel les/tous les *targets* (connus ou potentiels) des services de renseignement peuvent être automatiquement comparés aux données disponibles dans les banques de données techniques (provisoirement limitées à des systèmes intelligents de reconnaissance de plaques d'immatriculation). L'**analyse en temps réel** fait partie de ces possibilités. En d'autres termes, il s'agit d'un système de localisation permanente. Mais contrairement à la localisation via des métadonnées de communications, il s'agit ici d'une méthode ordinaire sans aucune limitation dans le temps. Le Comité estime que vu son impact (potentiel) sur la vie privée, ce moyen de collecte devrait au moins être considéré comme une méthode spécifique.

Par ailleurs, la réglementation proposée manque de clarté sur deux points. En fait, le Comité ne comprend pas bien la signification des passages suivants :

- *'La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique'.*
- *'Les critères d'évaluation visés à l'alinéa 1er, 2°, […] ne peuvent viser l'identification d'un individu […]*'.

Le projet d'article 16/4 § 6 L.R&S

Le projet d'article 16/4 § 6 L.R&S dispose que la réglementation visée à l'article 14 alinéa 2 L.R&S ne s'applique pas aux accès directs visés à l'article 16/4 L.R&S. Le Comité se demande si la réglementation visée à l'article 14 alinéa 3 L.R&S est elle aussi rendue caduque, et si le secret de l'enquête ne peut donc jamais être invoqué en la matière à l'égard des services de renseignement qui souhaitent consulter des images provenant de caméras. Le Comité estime que cette problématique doit être clarifiée.