Session ordinaire 2018-2019

MW/PR P.V. SID 16

Commission de la Sécurité intérieure et de la Défense

Procès-verbal de la réunion du 3 octobre 2019

Ordre du jour :

Présentation du projet de loi "Visupol"

*

Présents : Mme Nancy Arendt épouse Kemp, M. Carlo Back, M. André Bauler, M. François Benoy (en rempl. de M. Henri Kox), M. Eugène Berger (en rempl. de M. Gusty Graas), M. Yves Cruchten (en rempl. de M. Dan Biancalana), Mme Stéphanie Empain, M. Georges Engel, M. Léon Gloden, M. Marc Goergen, M. Max Hahn, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Georges Mischo, M. Laurent Mosar (en rempl. de Mme Diane Adehm)

M. David Wagner (en rempl. de M. Marc Baum, observateur délégué)

M. Gilles Roth, observateur

M. François Bausch, Ministre de la Sécurité intérieure

Ministère de la Sécurité intérieure :

Mme Béatrice Abondio, Mme Martine Schmit, Direction

Police grand-ducale :
M. Donat Donven, Directeur général adjoint, M. Patrick Even, Directeur Région Capitale, M. Luc Donckel, Directeur Technologies policières, Chargé de gestion de la Section Sécurité physique et multimédia

Inspection générale de la Police (IGP) :
Mme Monique Stirn, Inspecteur général, M. Vincent Fally, Inspecteur général adjoint

Mme Marianne Weycker, de l'Administration parlementaire

*

Présidence : Mme Stéphanie Empain, Présidente de la Commission

*

Présentation

Suite à quelques mots d'introduction de Madame la Présidente, Monsieur le Ministre fait savoir que la vidéosurveillance comporte trois volets : le premier est celui du recours à la vidéosurveillance, c'est-à-dire de la question de savoir quand et sous quelles conditions y avoir recours ; le deuxième volet est relatif à la protection des données, les conditions et la durée de conservation des enregistrements étant à déterminer clairement ; les droits des citoyens constituent le troisième volet, l'accès des citoyens aux données qui les concernent nécessitant une réglementation précise.

Le règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité, pris en exécution de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, manquait de précision sur certains points, notamment celui des cas et des conditions du recours à la vidéosurveillance (cf. supra, premier volet).

Avec la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, une nouvelle culture de traitement des données, avec une vue différente sur les droits des citoyens, a été introduite, se fondant sur la directive (UE) n° 2016/680[1]. Si la philosophie au début de l'entrée en vigueur de la loi de 2018 consistait à considérer celle-ci comme le cadre légal, dont les dispositions d'exécution seraient à prendre par les autorités concernées, parmi lesquelles la Police, Monsieur le Ministre a toujours préféré une législation spécifique déterminant clairement et de manière transparente les règles à appliquer, en particulier dans une matière sensible comme la vidéosurveillance. La Commission nationale pour la protection des données (CNPD) partage cette approche (cf. infra).

En amont de l'adoption de l'avant-projet de loi concernant la vidéosurveillance par le Gouvernement en conseil, Monsieur le Ministre tient à informer les députés sur le contenu et indique qu'il a aussi demandé à l'Inspection générale de la Police (IGP) d'élaborer un avis.

Une présentation PowerPoint est ensuite faite par le ministère.

Avant la réforme de 2018, la vidéosurveillance se basait sur la loi du 2 août 2002 précitée, dont l'article 17, paragraphe 1er, complété en 2007 par une lettre (d), disposait que :
« Art. 17. Autorisation par voie réglementaire
(1) Font l'objet d'un règlement grand-ducal :
(a) les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises.
Le règlement grand-ducal déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi,
(b) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et
(c) les traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol),
(d) la création et l'exploitation, aux fins et conditions visées sous (a), d'un système de vidéosurveillance des zones de sécurité. Est à considérer comme telle tout lieu accessible

[1] DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 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

au public qui par sa nature, sa situation, sa configuration ou sa fréquentation présente un risque accru d'accomplissement d'infractions pénales.
Les zones de sécurité sont fixées dans les conditions prévues par règlement grand-ducal. ».

Le règlement grand-ducal du 1er août 2007 précité autorisait la Police à mettre en œuvre un système de vidéosurveillance des zones de sécurité (article 1er). Suivant l'article 10, alinéa 1er, le ministre fixe les zones de sécurité par un règlement ministériel sur base d'une évaluation des risques émise par le Directeur général de la Police, de l'avis du Procureur d'État et de celui du comité de prévention communal ou intercommunal ; le ministre devait obligatoirement demander l'avis de ce comité, mais n'était pas obligé de l'attendre pour la détermination des zones. En vertu de l'alinéa 2 du même article : « Lors de la mise en service initiale du système de vidéosurveillance, les zones de sécurité à surveiller sont déterminées conformément à l'alinéa 1er pour une durée de deux ans. A l'expiration de ce délai, la vidéosurveillance de chaque zone de sécurité peut être prorogée annuellement par le ministre suite à une évaluation de l'utilité et de la nécessité de la vidéosurveillance de chaque zone de sécurité sur base de l'avis du directeur général de la police et du procureur d'Etat territorialement compétent, le comité de prévention communal ou intercommunal territorialement compétent ayant été demandé en son avis. ».

Par l'entrée en vigueur de la loi du 1er août 2018 précitée, la loi du 2 août 2002 fut abrogée et le règlement grand-ducal du 1er août 2007 était dépourvu de base légale. En parallèle a été adoptée la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, laquelle représente depuis son entrée en vigueur le 20 août 2018 le cadre général du traitement des données dans le domaine pénal.

Depuis août 2018, la vidéosurveillance n'est plus formellement prévue par la loi. La Police a réagi en émettant des prescriptions internes se basant sur les dispositions de la loi du 1er août 2018 (matière pénale), en vertu de l'avis du Conseil d'État, où celui-ci insiste sur la nécessité de conformer les traitements des données aux futures nouvelles prescriptions légales.

Sur sa propre initiative, la CNPD a rendu le 15 mars 2019 un avis sur la vidéosurveillance à des fins de sécurité publique, où elle constate que « comme tout dispositif de vidéosurveillance, VISUPOL est un instrument qui génère une surveillance permanente et un contrôle des individus. Par conséquent, ce dispositif de surveillance policière effectue une ingérence dans le droit à la vie privée et à la protection des données. Il est également susceptible d'entraver le droit à la non-discrimination et de limiter la libre circulation des personnes au sein de l'espace public. ». La CNPD voit la vidéosurveillance comme pouvant « générer de la discrimination et de la stigmatisation des individus se trouvant au sein des zones de sécurité ». Elle rappelle aussi que des limitations des droits des citoyens « sont possibles à condition d'être légalement prévues ». Selon la Cour européenne des droits de l'homme (CEDH), la simple existence d'une base légale n'est pas suffisante ; il faut en outre que celle-ci soit accessible et prévisible.

Dans son avis relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique – Délibération n°36/2019 du 15 mars 2019, la CNPD propose deux voies : « Ainsi, compte tenu de l'abrogation de la loi de 2002 et des règlements grand-ducaux sur lesquels le dispositif VISUPOL repose et les termes généraux dont fait preuve la loi relative aux missions de la Police grand-ducale, la CNPD suggère que les dispositions légales de cette dernière soient davantage précisées afin d'inclure VISUPOL dans son champ d'application.
Toutefois, la CNPD se demande s'il ne serait pas plus opportun que le Luxembourg se dote d'une loi spécifique encadrant l'installation et l'exploitation de dispositif de vidéosurveillance

dans l'espace public à des fins policières comme le font la France, la Belgique et l'Allemagne. ».

La voie d'une loi spécifique ayant été choisie, l'avant-projet de loi précise les conditions de mise en place des caméras, du traitement des images et les mesures protectrices des droits des citoyens. La mise en place des caméras nécessite une autorisation ministérielle délivrée sur base d'une analyse d'impact faite par le Directeur général de la Police, qui fournit par ailleurs les informations prévues par la loi justifiant la nécessité et la proportionnalité de la vidéosurveillance. À côté de l'avis du Procureur d'État, celui du bourgmestre est exigé, en remplacement de celui du comité de prévention communal ou intercommunal, puisque des représentants de la Police en font partie et qu'il est saugrenu que ceux-ci émettent un avis sur une analyse de leur Directeur général. L'autorisation ministérielle a une validité de trois ans et est publiée au Journal officiel.

Les caméras ne sont installées, comme ultime moyen, que dans des lieux qui présentent un risque particulier de commission, non plus d'infractions, mais spécifiquement de crimes ou délits ou d'atteintes à la sécurité des personnes ou des biens.

Concernant le traitement des images, celles-ci sont enregistrées sur support informatique avec l'indication du jour et de l'heure. Le recours à des techniques de focalisation et à des détections automatiques de situations est possible.

L'enregistrement, effectué en conformité avec la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, fait l'objet de certaines limites pour protéger les droits des citoyens :
- ne doivent pas être visualisés l'intérieur des lieux d'accès privés ni les entrées ; au cas où de tels endroits seraient enregistrés, ils devraient être masqués ;
- le public doit être informé sur place de la vidéosurveillance, ce qui est déjà le cas aujourd'hui ;
- à l'exception des données utilisées dans le cadre d'une enquête préliminaire ou d'une instruction judiciaire, les enregistrements sont effacés après deux mois ;
- les personnes habilitées à visionner les images en direct sont limitativement désignées par le Directeur général de la Police en sa qualité de responsable du traitement ;
- le visionnage en différé n'est possible que lorsqu'il est nécessaire pour l'exercice d'une mission précise de police judiciaire ou de police administrative et il est journalisé.

M. Laurent Mosar (CSV) s'étonne de la durée de conservation assez longue de deux mois, en songeant à l'exemple de la vidéosurveillance autour du stade, et souhaiterait en outre savoir ce qui se passe avec les données si l'affaire est classée.

Pour Monsieur le Ministre, il convient de mettre en place un automatisme similaire à celui pour les données du fichier central de la Police, lesquelles sont effacées sur feed-back des autorités judiciaires du classement de l'affaire.

Pour ce qui est de la durée de conservation de deux mois, l'orateur, en prenant l'exemple de la situation du quartier de la gare de la capitale, rappelle que la Police assure, à côté de la présence physique sur place, une mission d'observation. Il s'avère que l'observation doit pouvoir se prolonger souvent au-delà de deux mois avant de pouvoir intervenir.

Les représentants de la Police rendent attentif au fait que la conservation de données n'est toutefois pas destinée à servir de moyen d'observation ; l'autorisation du juge d'instruction est d'ailleurs nécessaire pour une observation prolongée. Le délai de conservation de deux mois a pour objet de permettre à une victime de porter plainte encore après un certain laps de temps, l'infraction pouvant ainsi être retracée jusqu'à deux mois après qu'elle a été

commise. Ce délai repose sur l'expérience des enquêteurs qui connaissent les raisons pour lesquelles des victimes ne portent pas plainte immédiatement. Le délai maximal de conservation des données de vidéosurveillance des bâtiments est en général d'un mois, celui des données enregistrées sur base des petites autorisations est d'une semaine.

M. Jean-Marie Halsdorf (CSV) indique que la vidéosurveillance produit les meilleurs résultats au visionnage en différé, d'où l'utilité du délai de conservation de deux mois. L'orateur obtient les réponses suivantes à ses questions d'ordre pratique : les personnes habilitées à visionner les images, les membres de l'unité VISUPOL, sont nominativement désignées par le Directeur général de la Police, de même que les autres personnes qui ont accès dans les bureaux de l'unité, à savoir les techniciens ou des membres de la police technique pour faire un retraçage dans le cadre d'une enquête ou instruction.

Parmi les personnes habilitées au visionnage en temps réel, il y a des civils, ce qui permet de faire intervenir les policiers davantage sur le terrain. Les personnes effectuant le visionnage en différé ne peuvent être désignées nominativement pour la raison notamment que la plainte peut être faite au commissariat du lieu de résidence ou encore de celui où l'infraction a été commise, le quartier de la gare en comptant déjà plusieurs. Le policier n'a alors d'accès que pour cette mission précise de police judiciaire et le visionnage est limité aux données y relatives.

Monsieur le Ministre mentionne que les détails feront l'objet d'un règlement grand-ducal et suggère aux députés de visiter l'unité VISUPOL.

Le principe général applicable en la matière étant celui de la proportionnalité, M. Gilles Roth (CSV) voit d'abord un problème de légalité du fait que les critères régissant le visionnage sont plus larges que les dispositions du Code de procédure pénale, en particulier de l'article 48-12 et suivants[2]. L'orateur est d'avis qu'il ne suffit pas de masquer les entrées privées, mais qu'elles ne doivent dès le départ pas être filmées, tout comme d'ailleurs les caméras installées sur un terrain privé ne doivent pas filmer l'espace public[3].

Ensuite, M. Roth considère le délai de conservation des données de deux mois également comme excessivement long, d'autant plus qu'il est prorogé en cas d'enquête préliminaire ou d'instruction judiciaire. Se pose la question de savoir s'il s'agit d'une enquête contre une personne déterminée ou s'il peut s'agir aussi d'une enquête contre X, sachant que, dans le second cas, des données de personnes non concernées sont conservées pendant toute cette durée et en plus à leur insu.

Finalement, l'orateur se réfère aux discussions menées en 2009 à la Chambre des Députés et souhaiterait savoir comment a été réglé le point litigieux de l'enregistrement des visages, lesquels ne devraient être filmés qu'à l'état figé.

Monsieur le Ministre renvoie à l'avis de la CNPD relatif à la vidéosurveillance (cf. supra) qui apporte de nombreuses clarifications. Quant à l'enregistrement des visages, il exprime son étonnement, déjà en ce qui concerne la faisabilité technique ; de plus, l'enregistrement par les bancomats serait alors illégal, pour ne mentionner que celui-ci. Les différentes questions posées pourront néanmoins être transmises au Commissaire du Gouvernement à la protection des données auprès de l'État, qui a également élaboré un avis.

[2] CPC, Livre I[er], Titre II, Chapitre VII – De l'observation (articles 48-12 – 48-16), introduit par la loi du 3 décembre 2009 portant
1) réglementation de quelques méthodes particulières de recherche
2) modification de certaines dispositions du Code pénal et du Code d'instruction criminelle

[3] Cf. travaux parlementaires dans le cadre du projet de loi 7184 devenu la loi du 1[er] août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données

La question essentielle qui se pose selon Monsieur le Ministre est celle de savoir combien de sécurité est souhaitée et donc combien de vie privée on est prêt à abandonner en faveur de la sécurité.

En réponse à une question de M. Marc Goergen (Piraten), un représentant de la Police explique que le « privacy masking » est effectué dès le début par la caméra et ne peut donc plus être enlevé par la suite. L'image enregistrée par la caméra et envoyée au server contient déjà le masquage privatif, de sorte que les entrées privées ne sont dès le départ pas reconnaissables. Une image réelle des parties privées n'est donc faite à aucun moment.

La présentation PowerPoint termine par le nouvel article 43*bis* à introduire dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale au Chapitre 5 – Traitement de données à caractère personnel. La loi précitée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale reste le cadre général en cette matière. Les auteurs se basent en outre sur l'avis de la CNPD sur le fichier central de la Police[4] pour régler de manière plus stricte les obligations qui incombent au responsable du traitement, faculté prévue par la directive (UE) n° 2016/680 - extrait de l'avis de la CNPD (pp. 26-27) : « Comme déjà soulevé, le législateur luxembourgeois a opté pour une approche très large de responsabilisation du responsable du traitement aux termes de la loi de transposition. Au regard de l'article 1.3 de la Directive, la CNPD estime qu'un encadrement légal plus strict des obligations de ce dernier augmenterait la qualité de la loi et par là, les garanties pour les personnes concernées.

Il en va de même de certains autres aspects de ce fichier comme les délais de conservation, la procédure d'accès restreinte à certaines données ou encore des garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables, en particulier les enfants.

Le législateur luxembourgeois pourrait ainsi utilement faire usage de la faculté laissée aux Etats membres telle que prévue au prédit article 1.3 qui dispose que : « La présente directive n'empêche pas les Etats membres de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et libertés de personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes ». Par l'adoption de la Directive, le législateur européen a procédé à une harmonisation minimale des règles applicable en la matière au niveau de l'Union européenne et les Etats membres ont la faculté de préciser davantage les règles dans leurs législations nationales respectives tout en respectant le cadre tracé par la Directive.

Rappelons que les précisions proposées ne s'inscriraient en principe pas dans la loi de transposition de la Directive, mais dans les lois spécifiques comme celle sur la Police ou celle relative à la protection de la jeunesse. ».

Par conséquent, le délai de conservation des données sera déterminé par la loi. En outre, un règlement grand-ducal précisera les mesures de sécurité du traitement des données, en application de l'article 28 de la loi précitée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Le règlement grand-ducal précité du 1er août 2007, pris en exécution de la loi précitée du 2 août 2002, était formulé de manière plus générale en reprenant les dispositions de la loi. En précisant les mesures de sécurité dans le règlement grand-ducal à prendre, elles seront publiées et le citoyen en aura connaissance.

[4] Avis de la Commission nationale pour la protection des données relatif au fichier central de la Police grand-ducale au regard de la législation sur la protection des données - Délibération n°45/2019 du 13 septembre 2019

Le même règlement déterminera aussi la procédure pour le droit d'accès des citoyens à leurs données.

Discussion

- Monsieur le Ministre assure que le règlement grand-ducal mentionné est en cours d'élaboration et sera mis à disposition des députés avant le vote sur la loi.

- M. Léon Gloden (CSV) s'intéresse au champ d'application de la future loi et souhaiterait savoir notamment si la vidéosurveillance d'une place publique ou d'un chemin public par une commune tombe dans ce champ ou sous le régime général (loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données).

Suivant les explications de Monsieur le Ministre, le régime général s'applique dans ce cas ; si, par la suite, il s'avère que l'aire surveillée répond aux critères retenus pour la vidéosurveillance par la Police, la procédure afférente peut être lancée.

- La mise en place des caméras nécessitant notamment l'avis du bourgmestre, en remplacement de celui du comité de prévention communal ou intercommunal, M. François Benoy (déi gréng) estime utile de réfléchir également à exiger l'avis du conseil communal en raison de l'impact que peut avoir la vidéosurveillance pour la commune.

Si Monsieur le Ministre peut se déclarer d'accord avec l'idée, il voudrait cependant limiter cette exigence à la vidéosurveillance en milieu urbain de la commune.

- M. Marc Goergen (Piraten) est informé que la reconnaissance faciale, à laquelle Monsieur le Ministre s'oppose radicalement, est exclue de la vidéosurveillance.

En réponse à sa question d'ordre technique au sujet de la transmission des images des caméras vers le serveur, un représentant de la Police fait savoir que la Police a son propre réseau où ne circulent que les données policières. En plus, VISUPOL dispose d'un réseau propre séparé sans connexion à Internet.

- M. David Wagener (déi Lénk) exprime ses doutes au sujet de l'exclusion de la reconnaissance faciale, en songeant à une certaine entreprise chinoise.

Selon des rapports indépendants et des articles parus à l'étranger, la vidéosurveillance ne présenterait que peu d'utilité, mais serait considérée comme gaspillage d'impôts. L'orateur souhaiterait dès lors savoir s'il existe au Luxembourg un rapport indépendant sur la vidéosurveillance, c'est-à-dire un rapport autre que l'avis élaboré par l'IGP seule, mais par de nombreux acteurs. Pour M. Wagener, l'élaboration commune par une multitude d'acteurs indépendants aboutit à un rapport réellement indépendant.

Une discussion sur le bien-fondé de la vidéosurveillance s'impose selon l'orateur, pour qui ce bien-fondé n'est pas donné. Se pose la question de savoir combien de cas sont élucidés au moyen de la vidéosurveillance. Les critères de détermination des zones pouvant être surveillées sont par ailleurs assez flous (« risque particulier de commission de crimes ou délits ou d'atteintes à la sécurité des personnes ou des biens »). M. Wagener exprime le souhait qu'une discussion approfondie soit menée sur la vidéosurveillance sur base d'études élaborées par de nombreux acteurs indépendants.

Pour Madame la Présidente, il est difficile de décider à partir de quel nombre d'acteurs un rapport peut être qualifié d'indépendant. Par ailleurs, un rapport fait par une multitude

d'acteurs indépendants aboutirait-il à d'autres conclusions, alors que la situation reste la même ?

M. Wagener précise que la vidéosurveillance se discute sous plusieurs perspectives : la perspective répressive, la perspective sociale, la perspective juridique ou encore celle de la réquisition des libertés publiques. En conséquence, un rapport ou avis élaboré par un seul acteur appartenant au domaine de la Police, sans mettre en doute la qualité du rapport ou avis, fera apparaître une seule perspective, alors que différents acteurs représentent différents points de vue.

Madame la Présidente rappelle que la future loi se basera non seulement sur l'avis de l'IGP, rendu sur demande du ministre, mais aussi sur le rapport de la CNPD, les deux instances tenant compte des intérêts et droits des citoyens.

- Le CSV note que les efforts vont dans la bonne direction. M. Laurent Mosar précise que certaines questions nécessitent néanmoins encore une réponse.

1) Quel régime légal est applicable aux caméras installées antérieurement à l'entrée en vigueur de la loi du 1er août 2018 (matière pénale) ? L'illégalité des images utilisées dans une affaire pénale peut-elle être invoquée devant les juridictions ?
2) Des clarifications s'imposent en matière de délais de conservation des données (cf. supra).
3) Un règlement grand-ducal devra déterminer de manière précise les personnes qui ont accès aux données.
4) Supposant que les enregistrements feront l'objet d'un fichier VISUPOL, il est essentiel de préciser le fonctionnement de ce fichier.

L'orateur peut se contenter d'une réponse au cours d'une prochaine réunion, le cas échéant, dans le cadre du dépôt du projet de loi.

- M. Carlo Back (déi gréng) souhaiterait être éclairé sur l'analyse d'impact, faite par le Directeur général de la Police, qui est nécessaire pour la délivrance de l'autorisation ministérielle pour la mise en place des caméras.

Suivant les explications de la part du ministère, l'analyse d'impact relative à la protection des données est une obligation imposée par la législation européenne relative à la protection des données.

- Au sujet du problème de légalité soulevé par M. Roth, Monsieur le Ministre considère comme techniquement très difficile de ne pas filmer les entrées privées dès le départ. S'il s'avérait que M. Roth a raison, il faudrait enlever toutes les caméras à proximité d'entrées privées. Cette question est à clarifier juridiquement.

Ad 2) et 3) : En ce qui concerne les délais de conservation des données, Monsieur le Ministre admet qu'il s'agit d'une question délicate, puisque plusieurs acteurs y ont un intérêt, en songeant aux enquêtes policières et judiciaires qui nécessitent un certain délai. L'appréciation des délais à retenir sera à faire en commun, la Police pouvant rassembler ses arguments et des exemples concrets en faveur du délai actuel de deux mois. Ce qui est clair pour l'orateur est que les données sont à radier après la clôture de l'enquête judiciaire. Une visite du service VISUPOL est à recommander pour obtenir aussi des informations sur le fonctionnement technique.

Un représentant de la Police explique que les données nécessaires dans le cadre d'une enquête sont mises sur CD-ROM en deux exemplaires par mesure de sécurité, dont l'un est transmis au parquet et l'autre gardé par l'enquêteur. Ces supports ne sont lisibles qu'au

moyen d'un lecteur VISUPOL. Suite à la clôture de l'instruction judiciaire, le CD-ROM est conservé dans le dossier avec les autres pièces à conviction tant que le dossier n'est pas détruit. À noter qu'un procès-verbal est dressé de chaque manipulation du système par un opérateur (indication des caméras, dont les images sont visionnées, de l'heure, des copies faites). La législation antérieure à 2018 prévoyait un délai de conservation des procès-verbaux de trois ans qui est considéré comme trop long ; un nouveau délai n'est cependant pas encore déterminé.

Monsieur le Ministre fait savoir qu'un règlement grand-ducal précisera les personnes qui ont accès aux données et les conditions à remplir pour avoir accès.

Le nombre de personnes habilitées à visionner les images s'élève actuellement à 36. Il s'agit d'opérateurs (policiers et civils), d'enquêteurs et de personnel technique.

À la question de l'utilité de la vidéosurveillance, les réponses varient largement. Monsieur le Ministre a une approche personnelle nuancée. Insistant sur une législation précise en la matière, l'orateur constate que la vidéosurveillance ne présente quasiment pas d'utilité au niveau de la prévention. Si elle a certes un certain effet dissuasif, son efficacité se révèle surtout dans l'élucidation d'infractions, en songeant en particulier à la zone Gare.

Ad 1) : L'avis à émettre par l'IGP ne se limitera pas à l'analyse des résultats de la vidéosurveillance jusqu'à présent et de son opportunité, mais s'intéressera entre autres à l'opinion des habitants des zones filmées. En attendant cet avis, il convient de légiférer déjà pour donner une base légale solide à la vidéosurveillance.

Concernant le risque que l'illégalité des images enregistrées par les caméras installées antérieurement à l'entrée en vigueur de la loi du 1er août 2018 (matière pénale) soit invoquée, Monsieur le Ministre rappelle que l'approche de cinq pays, dont le Luxembourg, consiste à dire que la loi de transposition de la directive (UE) n° 2016/680 constitue le cadre légal, dont les dispositions d'exécution seraient à prendre par les autorités concernées (cf. supra). Comme il l'a déjà précisé plus haut, Monsieur le Ministre s'est toujours prononcé pour une législation spécifique déterminant clairement les règles à appliquer, ce système, en parlant du domaine de la vidéosurveillance, procurant aussi à la Police une plus grande sécurité et protection dans son travail. Cette approche est partagée par la CNPD.

- La commission accueille favorablement la proposition ministérielle de rendre visite au service VISUPOL.

Le Secrétaire-administrateur,
Marianne Weycker

La Présidente de la Commission de la Sécurité intérieure et de la Défense,
Stéphanie Empain

Annexe : La vidéosurveillance à des fins policières

LA VIDÉOSURVEILLANCE A DES FINS POLICIÈRES

Commission de la Sécurité intérieure et de la Défense

3 octobre 2019

Cadre légal de la vidéosurveillance avant le 20 août 2018

- Art. 17(d) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel telle que modifiée en 2007

- Règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité

Art. 17 (d) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

- Autorisation par RGD de la création et de l'exploitation d'un système de vidéosurveillance des zones de sécurité à des fins de prévention, de recherche et de constatation d'infractions pénales
- Loi définit les zones de sécurité comme les lieux accessibles au public qui par leur nature, leur situation, leur configuration ou leur fréquentation présentent un risque accru d'accomplissement d'infractions pénales
- Relègue au règlement grand-ducal:
  - Détermination du responsable du traitement
  - Condition de légitimité du traitement
  - Finalités du traitement
  - Catégories de personnes concernées
  - Données traitées et origine des données
  - Destinataires des données
  - Mesures de sécurité à prendre
  - Conditions de fixation des zones de sécurité

- Autorise la Police à mettre en œuvre un système de VS des zones de sécurité
- Désignation des zones par le Ministre sur base d'une évaluation des risques du DGP et des avis du procureur d'Etat et du comité de prévention communal
- Validité initiale de la désignation: 2 ans, puis prorogation annuelle

Cadre légal de la vidéosurveillance depuis le 20 août 2018

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Abrogation de la loi de 2002 par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données

- La loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale constitue désormais le cadre juridique pour les traitements de données à caractère personnel en matière pénale

- La vidéosurveillance n'est plus formellement prévue par la loi

- La Police, en tant que responsable du traitement a émis des prescriptions internes encadrant le système VISUPOL sur base des dispositions de la loi du 1er août 2018

Avis de la CNPD du 15 mars 2019 sur l'utilisation de la vidéosurveillance à des fins de sécurité publique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- VISUPOL génère une surveillance permanente et un contrôle des individus
- VISUPOL a un impact sur les droits fondamentaux (limitation du droit à la vie privée, discrimination et stigmatisation des personnes se trouvant dans une zone surveillée, limitation du droit à la libre circulation)
- Une ingérence dans les droits fondamentaux est possible à condition (1) d'être prévue par la loi et (2) que la loi soit accessible et prévisible
- 2 options:
  - 1. préciser la loi du 18 juillet 2018 sur la Police grand-ducale
  - 2. élaborer une loi spécifique

Création d'un nouveau cadre légal : questions à trancher

- Elaborer une nouvelle loi ou intégrer la vidéosurveillance dans une loi existante?
- Quelles dispositions à inscrire dans la loi?
- Prévoir des mesures d'exécution par règlement grand-ducal?

Contenu de l'avant-projet de loi

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Conditions à la mise en place de caméras de VS
- Traitement des images
- Mesures protectrices des droits des citoyens

Conditions à la mise en place de caméras de vidéosurveillance (1)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

➢ Une autorisation ministérielle

- Délivrée sur base d'une analyse d'impact réalisée par le DGP et d'un certain nombre d'informations et critères, énumérés par la loi, qui sont destinés à permettre au ministre d'évaluer la nécessité et la proportionnalité de la VS
- Avis du procureur d'Etat et du bourgmestre territorialement compétents
- Autorisation valable pour une durée de 3 ans renouvelables
- Autorisation publiée au JOLU

Conditions à la mise en place de caméras de vidéosurveillance (2)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- **Des lieux qui présentent un risque particulier de commission de crimes ou délits ou d'atteintes à la sécurité des personnes ou des biens**

  - les lieux où sont commis, de manière répétée, les mêmes types de crimes ou de délits
  - les lieux qui par leur configuration sont de nature à favoriser la commission de certains types de crimes ou délits, à condition que les autres moyens mis en œuvre pour en empêcher la commission se sont avérés inefficaces
  - les alentours et abords des infrastructures où sont organisés régulièrement des évènements d'envergure nationale ou internationale
  - les lieux qui par leur nature rassemblent un grand nombre de personnes

Traitement des images

- Prise d'images et enregistrement des images + jour et heure sur support informatique

- Possibilité de recourir à des techniques de focalisation et à des détections automatiques de situations (≠ reconnaissance faciale)

Mesures protectrices des droits des citoyens

- Pas de visualisation des intérieurs des lieux d'accès privé ni des entrées
- Information du public de la présence de la VS
- Effacement des données après 2 mois (sauf le cas d'une enquête préliminaire ou d'une instruction judiciaire)
- Limitation du cercle de personnes habilitées à visionner les images en temps réel
- Limitation du visionnage en différé à l'exercice d'une mission précise de police judiciaire ou de police administrative (+ journalisation)

Le nouvel article 43*bis* et la loi du 1er août 2018 sur la protection des données en matière pénale

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Loi du 1.8.2018 constitue le cadre général du traitement de données en matière pénale, y compris les données traitées dans le cadre de la vidéosurveillance
- La présente loi encadre plus strictement les obligations incombant au responsable du traitement en vertu de la loi du 1.8.2018, à savoir:
  - La loi fixe le délai de conservation et non le responsable du traitement
  - Un règlement grand-ducal devra déterminer les mesures techniques et organisationnelles que la Police doit mettre en œuvre en application de l'article 28 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et règle les modalités d'exercice du droit d'accès prévu à l'article 13 de la même loi.