Avis de la Commission nationale pour la protection des données relatif au recours à la vidéosurveillance par les communes

Délibération n°39/2019 du 10 mai 2019

Conformément à l'article 57, paragraphe 1er lettre c) du règlement n°2016/679 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 (règlement général sur la protection des données (ci- après désigné « RGPD »), auquel se réfère l'article 7 de 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 Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») « conseille, conformément au droit de l'Etat membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».

Eu égard à la mission de conseil qui lui est attribuée, mais également suite à la requête de Madame la Ministre de l'Intérieur concernant les conditions d'installations de caméras de vidéosurveillance au sein des communes et face aux interrogations des bourgmestres à ce sujet, la Commission nationale rend un avis circonstancié quant au recours à la vidéosurveillance par les communes.

A titre liminaire, la CNPD constate que les communes, dans leurs demandes d'informations quant à l'installation de dispositifs de vidéosurveillance dans l'espace public, font référence à l'ancien régime de protection des données. Un bref retour en arrière est donc nécessaire afin de comprendre les tenants et les aboutissants du cadre légal actuellement en vigueur.

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, en particulier les articles 10 et 11, prévoyait des dispositions spécifiques relatives à la surveillance. L'article 14 de cette loi prévoyait quant à lui, l'obligation de demander une autorisation auprès de la CNPD avant toutes installations de dispositifs de vidéosurveillance. L'article 17 de cette même loi était le fondement légal de la surveillance de l'espace public effectuée par la Police grand-ducale.

Aujourd'hui, la saisie de la CNPD par Madame la Ministre de l'Intérieur intervient au lendemain de l'entrée en application du nouveau « paquet protection des données » composé d'un règlement général pour la protection des données[1] (ci-après désigné « RGPD ») et d'une directive relative à la protection des données dans les domaines relatifs à la police et la justice[2] (ci-après désignée « la directive police-justice »). Ces deux textes ont des champs d'application distincts mais néanmoins complémentaires.

Le RGPD est directement applicable dans la législation luxembourgeoise. 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 a abrogé la loi modifiée du 2 août 2002 relative

[1] 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, JO L119, 4.5.2016, p.1-88.

[2] Directive (UE) n° 2016/680 du 27 avril 2016 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention 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, JO L119, 4.5.2016, p. 89-131.

à la protection des personnes à l'égard du traitement des données à caractère personnel. La nouvelle législation a supprimé l'obligation pour les responsables de traitement de données à caractère personnel d'effectuer une demande d'autorisation à la CNPD avant l'installation de dispositifs de vidéosurveillance. Les communes, en tant que responsables de traitement[3] sont à présent tenues de respecter les principes[4] et obligations consacrés par le RGPD lorsqu'elles mettent en place des systèmes de vidéosurveillance.

A ce titre et suite à l'entrée en vigueur de la nouvelle législation, la CNPD a publié au mois d'août 2018 des lignes directrices en matière de vidéosurveillance (ci-après désignées « les lignes directrices »). Sans vouloir prétendre à l'exhaustivité, la CNPD y a rappelé certains principes et certaines obligations applicables en matière de vidéosurveillance. Par conséquent, les communes peuvent se référer aux lignes directrices dont une copie est fournie en annexe[5] du présent avis, afin d'avoir un aperçu des règles applicables en la matière.

Afin de bien saisir les enjeux que soulèvent l'installation et l'exploitation des dispositifs de vidéosurveillance au sein des communes et les problématiques qui en émanent, il y a lieu d'effectuer une distinction entre les lieux surveillés d'une part, et les finalités poursuivies par le responsable de traitement lors du recours auxdits dispositifs d'autre part. Ces enjeux et problématiques peuvent être mis en lumière à travers trois exemples développés ci-dessous.

Lorsqu'une commune souhaite surveiller un bâtiment ou d'autres installations communales à des fins de protection des biens et/ou de sécurité des usagers, une telle surveillance intervient dans le cadre des missions « classiques » reconnues à celle-ci. Avant l'entrée en application du RGPD et sous l'égide de la loi de 2002, la CNPD autorisait la surveillance de ces zones sous réserve du respect de certaines conditions et obligations. Aujourd'hui, la commune est tenue de respecter les principes et les obligations du RGPD, qui d'ailleurs, n'ont pas changé par rapport à l'ancienne législation. A titre d'exemples, la CNPD considère que l'installation d'un dispositif de vidéosurveillance est en principe proportionnée aux entrées et aux sorties de bâtiments, aux alentours immédiats de ces derniers, dans des locaux de stockage, aux zones de livraisons et de chargements[6] etc. Le caractère proportionné réside dans le fait que les zones surveillées sont restreintes et les personnes qui y sont présentes telles que les visiteurs, les clients ou encore les employés, ne sont pas soumis à une surveillance permanente.

Lorsqu'une commune souhaite installer des dispositifs de vidéosurveillance au sein de l'espace public, la zone surveillée est en principe plus étendue. Le champ de vision du dispositif couvre des surfaces beaucoup plus grandes telles que des places publiques, des parcs, des aires de jeux ouvertes à tous ou encore des rues. Avant l'entrée en application du RGPD et conformément à la loi de 2002, la CNPD n'autorisait pas la surveillance de ces zones considérant que la protection des intérêts des citoyens prévalait sur la protection des biens et la sécurité des usagers. En ce qui concerne les aires de jeux, en particulier, la CNPD a toujours considéré que l'installation et l'exploitation de vidéosurveillance étaient attentatoire à la vie privée puisqu'il s'agissait là d'espaces de vie, de loisirs et de récréation dans lesquels l'on pouvait légitimement s'attendre à ne pas être filmé et surveillé en permanence pendant le temps de présence dans ces espaces. Sous l'égide du cadre légal actuel, la position de la CNPD reste en principe inchangée. Dans ses lignes directrices et conformément au RGPD, la

---

[3] Une définition de ce qu'est un responsable de traitement est donnée à l'article 3. 7) du 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, JO L119, 4.5.2016, p.1-88.

[4] *Ibidem*, article 5 et suivants.

[5] Annexe I.

[6] Lignes directrices en matière de vidéosurveillance, p.8.

CNPD considère qu'au sein de ces zones, l'installation de caméras est disproportionnée par rapport aux buts poursuivis. En effet, la surveillance qui en émane porte sur un nombre conséquent d'individus qui circulent au sein de l'espace public et cette surveillance n'est pas limitée dans le temps.

En outre, la CNPD constate qu'il ressort des demandes d'avis de la part des communes que celles-ci souhaitent installer des dispositifs de vidéosurveillance à des fins de prévention et de détection d'infractions pénales. Il apparaît en effet que ces dernières ont l'intention de lutter contre des actes de délinquance, de vandalisme etc., d'autant plus que certaines communes ont manifesté leur souhait d'être reliées au système VISUPOL, exploité par la Police grand-ducale actuellement limité au seul territoire de la Ville de Luxembourg. Or, dans une telle hypothèse, c'est un autre régime légal qui s'applique en matière de protection des données. Il s'agit en effet 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[7]. Cette loi transpose la directive police-justice[8] précitée en droit national.

A cet égard, la Commission nationale pour la protection des données a rendu le 15 mars 2019 un avis relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique[9] dont une copie est également fournie en annexe[10]. Celui-ci peut être très utile aux communes souhaitant installer un dispositif de vidéosurveillance à des fins de sécurité publique et doit être lu de concert avec les présents développements.

La CNPD souhaite attirer l'attention sur le fait que la finalité du traitement poursuivie par le responsable du traitement, en l'espèce la commune, doit entrer dans le champ de compétence de celui-ci. Comme l'indique le Groupe de travail « article 29 » : « il faudra tenir compte des fonctions publiques qui ne peuvent être exercées, aux termes de la loi, que par des organismes spécifiques non administratifs tels que, en particulier, des organismes de police et/ou l'autorité judiciaire »[11]. Autrement dit, une commune ne peut outrepasser ses compétences et installer un système de vidéosurveillance pour une finalité qui relève des compétences de la Police grand-ducale.

La CNPD constate cependant que si la loi communale et la loi sur la Police grand-ducale mettent en exergue les interactions entre la police et les bourgmestres, aucune des deux ne précisent les compétences des bourgmestres en matière de police. En effet, la loi communale renseigne sur les attributions des bourgmestres[12] et sur l'interaction entre ces derniers et la Police grand-ducale[13]. La loi du 18 juillet 2018 sur la Police grand-ducale[14] (ci-après désignée

---

[7] 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 portant modification de certaines lois.

[8] Directive (UE) n° 2016/680 du 27 avril 2016 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention 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, JO L119, 4.5.2016, p. 89-131.

[9] Avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique, Délibération n°36/2019 du 15 mars 2019.

[10] Annexe II.

[11] Avis 4/2004 du groupe de travail « Article 29 » sur le traitement des données à caractère personnel au moyen de la vidéosurveillance, p.14, disponible à l'adresse suivante : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp089_fr.pdf

[12] Loi communale du 13 décembre 1988, article 67.

[13] *Ibidem*, article 68.

[14] Loi du 18 juillet 2018 sur la Police grand-ducale et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination

« loi sur la Police grand-ducale ») quant à elle, fait également part des interactions entre la police et les autorités communales. Il y est fait état des relations étroites entre les bourgmestres et les directeurs des régions de Police et les chefs des commissariats de police[15]. Or, ces dispositions légales ne permettent pas de délimiter clairement les compétences des bourgmestres de celles de la Police grand-ducale.

La CNPD souhaite également relever qu'un tel manque de précision se conjugue avec l'absence de base légale spécifique en matière de vidéosurveillance ne permettant pas de remplir les impératifs de prévisibilité et de qualité de la loi tels qu'ils sont consacrés par le droit de l'Union européenne et la jurisprudence des hautes juridictions européennes[16].

Conclusion

Dans son avis précité du 15 mars 2019, la CNPD est venue à la conclusion que, quel que soit le responsable du traitement, qu'il s'agisse d'une commune ou de la Police grand-ducale, les conditions et les modalités de mise en place de dispositifs de vidéosurveillance dans les espaces et lieux publics à des fins de sécurité publique devraient être précisés dans un cadre légal spécifique à l'instar d'autres pays européens comme par exemple la France, la Belgique et l'Allemagne. Dans ce contexte, elle a également salué la récente déclaration du Ministre de la sécurité intérieure qui considère « *qu'il est opportun de réfléchir à la mise en place d'un cadre légal spécifique pour l'installation future de caméras de surveillance* »[17].

Dans le cadre du présent avis, la CNPD ne peut que réitérer sa recommandation au gouvernement d'introduire en ce sens un cadre législatif spécifique, lequel pourrait intégrer et clarifier les interactions et les compétences respectives des bourgmestres et de la Police grand-ducale.

---

de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; 3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ; 5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation :
1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. La loi du 23 juillet 1952 concernant l'organisation militaire ; 2. Le code d'instruction criminelle ; 3. La loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police

[15] *Ibidem*, articles 35 et 36.

[16] Les développements concernant les critères de prévisibilité et de qualité de la loi peuvent être retrouvés au sein de l'avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique, Délibération n°36/2019 du 15 mars 2019, pages 7 et suivantes.

[17] Communiqué par le ministère de la Sécurité intérieure du 12/03/2019, disponible à la page : https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/03-mars/12-bausch-videoprotection.html, consultée pour la dernière fois le 12/03/2019.

Ainsi décidé à Esch-sur-Alzette en date du 10 mai 2019.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann	Marc Lemmer
Présidente	Commissaire	Commissaire	Commissaire

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Le Règlement Général sur la Protection des Données

Lignes directrices en matière de vidéosurveillance

Contenu

Introduction

Depuis le 25 mai 2018, le **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 (ci-après : « le RGPD »), trouve application.

Contrairement à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (abrogée 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), le RGPD ne définit pas la notion de « surveillance ». De plus, une des conséquences directes du RGPD est qu'il n'est **plus nécessaire de demander l'autorisation** préalable de la CNPD pour installer un système de vidéosurveillance.

Si l'obligation de demander une autorisation préalable à la CNPD a disparu, les responsables du traitement sont maintenant obligés de tenir un registre des traitements de données à caractère personnel qui sont effectués sous leur responsabilité et ce, conformément à l'article 30 du RGPD. Le traitement de données à caractère personnel découlant de la vidéosurveillance devra dès lors y figurer et inclure les informations exigées par l'article 30 du RGPD.

Sans vouloir prétendre à l'exhaustivité, la CNPD tient en outre à **rappeler certains principes et certaines obligations** applicables en matière de vidéosurveillance.

1. Principe de licéité du traitement

Tout traitement de données à caractère personnel doit reposer sur une des conditions de licéité limitativement énumérées à l'article 6.1 (lettres a) - f)) du RGPD. Dans le cadre d'un système de vidéosurveillance, la condition de licéité la plus appropriée sera, de façon générale, que le traitement est nécessaire aux fins des intérêts légitimes du responsable de traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la ou des personne(s) soumise(s) à la vidéosurveillance (article 6.1, f) du RGPD).

Attention : en principe, le consentement ne constitue pas une base de licéité appropriée en matière de vidéosurveillance.

2. Principe de finalité

Conformément à l'article 5.1, b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

A titre d'exemple, la surveillance par caméras vidéo peut avoir pour finalités :

- de sécuriser les accès au bâtiment ;
- d'assurer la sécurité du personnel et des clients ;
- de détecter et d'identifier des comportements potentiellement suspects ou dangereux susceptibles de provoquer des accidents ou incidents ;
- de repérer avec précision l'origine d'un incident ;
- de protéger les biens (bâtiments, installations, matériel, marchandes, liquidités, etc.) ;
- d'organiser et d'encadrer une évacuation rapide des personnes en cas d'incident ;
- de pouvoir alerter en temps utile les services de secours, d'incendie ou des forces de l'ordre ainsi que de faciliter leur intervention.
- ...

Avant l'installation d'un système de vidéosurveillance, le responsable du traitement devra définir, de manière précise, la ou les finalités qu'il souhaite atteindre en recourant à un tel système, et ne pourra pas l'utiliser ensuite à d'autres fins. L'exemple repris ci-dessous au point 4.3 des présentes lignes directrices illustre ce principe de limitation des finalités.

3. Principe de transparence

Tout responsable du traitement est obligé d'informer les personnes concernées du traitement de données à caractère personnel qu'il met en œuvre. Cette information doit répondre aux exigences des articles 12 et 13 du RGPD. Elle peut notamment être communiquée par l'apposition de panneaux d'affichages et de pictogrammes aux endroits soumis à la vidéosurveillance, en plus d'une notice d'information plus détaillée publiée, par exemple, sur le site internet du responsable du traitement.

Attention : Le principe de transparence, tel que prévu à l'article 5, paragraphe 1, lettre a) du RGPD, implique que des mesures de surveillance **cachées** ne peuvent jamais être mises en œuvre par un responsable du traitement.

4. Principe de nécessité et de proportionnalité (minimisation des données)

Le principe de minimisation des données en matière de vidéosurveillance implique qu'il ne doit être filmé que ce qui apparait strictement nécessaire pour atteindre la/les finalité(s) poursuivie(s) (« données adéquates, pertinentes et limitées à ce qui est nécessaire ») et que les opérations de traitement ne doivent pas être disproportionnées.

Au regard de la jurisprudence découlant des décisions d'autorisation précédemment adoptées par la CNPD et de décisions judiciaires, cette dernière a dégagé, en termes de proportionnalité, certains principes imposant des conditions et exigences lors de l'utilisation de la vidéosurveillance. Ceux-ci sont expliqués dans les présentes lignes directrices.

A titre illustratif, un aperçu de zones dans lesquelles la CNPD estime qu'un système de vidéosurveillance peut-être ou non problématique figure ci-dessous au point 4.5. Toutefois, il y a lieu d'effectuer une analyse de la situation au cas par cas afin d'analyser la nécessité et la proportionnalité d'une vidéosurveillance, notamment au regard de critères tels que, par exemple, la nature du lieu à placer sous vidéosurveillance, sa situation, sa configuration ou sa fréquentation.

4.1. Champ de vision limité des caméras filmant les accès intérieurs, extérieurs ou les alentours d'un bâtiment ou d'un site

Les caméras destinées à surveiller un lieu d'accès (entrée et sortie, seuil, perron, porte, auvent, hall, etc.) doivent avoir un champ de vision limité à la surface strictement nécessaire pour visualiser les personnes s'apprêtant à y accéder ; celles qui filment des accès extérieurs ne doivent pas baliser toute la largeur d'un trottoir longeant, le cas échéant, le bâtiment ou les voies publiques adjacentes.

De même, les caméras extérieures installées aux abords ou alentours d'un bâtiment doivent être configurées de façon à ne pas capter la voie publique, ni les abords, entrées, accès et intérieurs d'autres bâtiments avoisinants rentrant éventuellement dans leur champ de vision.

En fonction de la configuration des lieux, il est parfois impossible d'installer une caméra qui ne comprendrait pas dans son champ de vision une partie de la voie publique, abords, entrées, accès et intérieurs d'autres bâtiments. Dans un tel cas, la CNPD estime que le responsable du traitement doit mettre en place des techniques de masquages ou de floutage afin de limiter le champ de vision à sa propriété.

4.2. Surveillance permanente et continue

Une surveillance permanente de personnes non salariées n'est pas toujours admise. Par exemple, la CNPD estime qu'il est disproportionné de filmer l'intérieur d'une salle de restauration comprenant des tables de consommation. Il en va de même de la terrasse ou du comptoir d'un café. En effet, même si un certain risque de vol ou de vandalisme peut exister dans pareils lieux, elle estime que les clients présents seront, de façon permanente, soumis à la vidéosurveillance alors qu'ils choisissent un restaurant ou un café comme lieu de rencontre pour passer un bon moment autour d'un repas, pour communiquer, se divertir ou se détendre. Les clients qui restent dans ce type de lieu pendant un laps de temps plus ou moins long doivent pouvoir légitimement s'attendre à ne pas être filmés pendant ces moments privés. L'utilisation des caméras dans la salle de restauration comprenant les tables de

consommation est susceptible de filmer le comportement de chaque client assis à une table et peut créer une gêne voire une pression psychologique pour les clients qui se sentent observés tout au long de leur présence dans le restaurant. Une telle surveillance permanente est dès lors à considérer comme disproportionnée à la finalité recherchée et constitue une atteinte à la sphère privée du client.

Sur le lieu de travail, les salariés ont en principe le droit de ne pas être soumis à une surveillance continue et permanente.

En effet, le respect du principe de proportionnalité implique que l'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié. Le respect de ce principe exige que, par exemple, doivent être évitées les surveillances automatiques et continues des salariés.

Ainsi par exemple, l'exploitant d'un restaurant ne pourrait surveiller ses salariés à l'intérieur de la cuisine, en invoquant la protection de ses biens. Les salariés seraient soumis à la vidéosurveillance de façon quasi permanente et il est évident qu'une pareille surveillance peut créer une pression psychologique non négligeable pour les salariés qui se sentent et se savent observés, d'autant plus que les mesures de surveillance perdurent dans le temps. Il en va de même, par exemple, de la mise sous vidéosurveillance de l'intérieur d'un bureau, d'un open-space, ou encore d'un atelier dans lequel travaillent en permanence un ou plusieurs salariés. Une surveillance permanente est considérée comme disproportionnée à la finalité recherchée et constitue une atteinte excessive à la sphère privée du salarié occupé à son poste de travail. Dans ce cas, les droits et libertés fondamentaux des salariés doivent prévaloir sur les intérêts légitimes poursuivis par l'employeur.

Afin d'éviter une surveillance permanente et continue, le responsable du traitement doit limiter le champ de vision des caméras à la seule surface nécessaire pour atteindre les finalités poursuivies.

Ainsi, à titre d'exemple, la surveillance par caméra d'une caisse d'un magasin peut avoir pour finalités de protéger les biens du responsable du traitement contre les actes de vol commis par ses salariés ou par un client/usager et d'assurer la sécurité de son personnel. Toutefois, afin de de ne pas porter atteinte à la vie privée des salariés, la caméra devra être configurée de façon à ce que les salariés présents derrière un comptoir-caisse ne soient pas ciblés, en orientant son champ de vision vers la caisse elle-même et l'avant du comptoir, c'est-à-dire l'espace d'attente des clients se trouvant devant le comptoir, et ce, en vue de permettre l'identification des auteurs d'agressions, par exemple.

4.3. Surveillance des prestations et des comportements des salariés

La CNPD estime que la vidéosurveillance ne doit pas servir à observer le comportement et les performances des membres du personnel du responsable du traitement en dehors des finalités pour lesquelles elle a été mise en place.

Ainsi, un employeur a le droit d'utiliser les images d'un salarié commettant un vol de marchandises et qui proviennent d'un système de vidéosurveillance utilisé pour une finalité de protection des biens. Or, il n'a pas le droit de prendre des mesures à l'encontre d'un salarié lorsque, au goût de l'employeur, le salarié discute trop longtemps avec un client ou un collègue de travail et que ce comportement est enregistré par le système de vidéosurveillance. Ceci constituerait un détournement de finalité interdit par le RGPD.

4.4. Les endroits réservés aux salariés pour un usage privé

La CNPD estime que les caméras de surveillance ne doivent pas filmer les endroits réservés aux salariés pour un usage privé ou qui ne sont pas destinés à l'accomplissement de tâches de travail, comme par exemple les toilettes, les vestiaires, le coin fumeurs, les zones de repos, le local mis à la disposition de la délégation du personnel, la cuisine/kitchenette, etc.

4.5. Exemples de zones de vidéosurveillance

Les exemples de zones ci-dessous doivent être lus et considérés ensemble avec les points 4.1 à 4.4 ci-dessus.

A. Zones où l'installation d'une vidéosurveillance est en principe proportionnée :

- toutes sortes d'accès, sauf exception (les champs de vision des caméras doivent être limités à la surface strictement nécessaire) ;
- des locaux de stockage de marchandises / les réserves / les entrepôts / les halls ou hangars de stockage (sauf si des salariés sont affectés en permanence à travailler dans le stock, comme p.ex. des magasiniers) ;
- des espaces ou surfaces de vente d'un commerce / les rayons d'un magasin / une galerie marchande / un espace d'exposition / un espace de vente et de conseil (sauf des postes de travail permanents derrière un comptoir) ;
- un parking (intérieur / extérieur / souterrain) ;
- des zones de livraisons ou de chargement / les quais de livraison et de déchargement ;
- une salle informatique / une salle de serveurs ;
- des couloirs (sauf hôtels – situation particulière) ;
- une station de lavage automatique de véhicules / un carwash ;
- une pompe à essence ;
- un coffre-fort / un local sécurisé / des consignes automatiques ;
- des locaux de transport de fonds / un local de convoyeurs de fonds / un local fourgon ;
- des machines de production (uniquement machines) ;
- des installations purement techniques ;
- le local technique d'un bâtiment / un local de maintenance / un local des compteurs d'une copropriété ;
- des locaux d'archives ;
- des distributeurs automatiques de billets / un guichet automatique bancaire.

B. Zones où l'installation d'une vidéosurveillance est en principe disproportionnée:

- une voie publique / un trottoir (sauf exception en fonction de la configuration spécifique des lieux ; le champ de vision ne peut cependant englober qu'une partie extrêmement limitée de la voie publique) ;
- l'intérieur d'une zone de consommation d'un établissement de restauration, d'un débit de boisson, d'un night-club, etc. (salle de restauration, comptoir de consommation, terrasse, cantine/cafeteria, etc.) ;
- l'intérieur d'une cuisine ;
- l'entrée privative d'une habitation dans un immeuble en copropriété ;
- un terrain ou un bâtiment avoisinant ;
- l'intérieur d'un bureau comprenant un poste de travail permanent ;
- une salle de repos ou de séjour ;
- les zones d'entrainement dans une salle de sport ;
- des toilettes / des sanitaires / des douches ;
- un bureau de la représentation du personnel ;
- une kitchenette / un espace fumeur;
- un vestiaire / une salle de casiers ;
- l'atelier d'un garage / un atelier de montage et démontage de pneus / un atelier de production / un atelier de travail ;
- l'espace de coiffage d'un salon de coiffure ;
- l'espace de jeu d'une crèche.

C. Zones où le caractère proportionné ou non d'une vidéosurveillance dépend des circonstances de l'espèce et des mesures mises en place afin de garantir le respect de la vie privée

La mise sous vidéosurveillance des zones listées ci-dessous peut être admise dans certains cas, et non admise dans d'autres cas. Le caractère proportionné ou non de la vidéosurveillance de pareilles zones dépendra des circonstances de l'espèce, comme par exemple la nature, la situation ou la configuration des lieux, la nature de l'activité exercée par le responsable du traitement et les risques inhérents à cette activité, etc. Elle dépendra également des mesures prises par le responsable du traitement afin de rendre la vidéosurveillance moins attentatoire à la vie privée des personnes concernées (par exemple, limitation du champ de vision des caméras, utilisation de techniques de masquage/floutage, etc.). Une analyse au cas par cas doit être réalisée par le responsable du traitement, au besoin avec l'aide de la CNPD.

- les alentours d'un bâtiment ;
- une salle d'attente ;
- des guichets ;

- un comptoir d'accueil / un comptoir de réception ;
- des caisses
- une salle de comptage de caisses / une salle de traitement des fonds ;
- les parties communes d'un immeuble en copropriété;
- la cour de récréation d'une école (et alentours) ;
- une piscine ;
- le toit d'un bâtiment ;
- une salle de réunion.

4.6. Le traitement des sons associés aux images

Une surveillance au moyen de caméras vidéo ne doit porter que sur des images à l'exclusion de sons. En effet, l'écoute en direct ainsi que l'enregistrement du son associé aux images rend la vidéosurveillance encore plus intrusive et est à considérer comme disproportionné.

4.7. Durée de conservation des images

Le RGPD dispose que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Pour ce qui est de la vidéosurveillance, la CNPD estime que les images peuvent être conservées en principe jusqu'à 8 jours.

Le responsable du traitement peut exceptionnellement conserver les images pour une durée de 30 jours. Toutefois, il y a lieu d'indiquer les raisons qui justifient une telle durée de conservation dans le registre des traitements.

Une durée de conservation supérieure à 30 jours est généralement considérée comme étant disproportionnée.

En cas d'incident ou d'infraction, les images peuvent être conservées au-delà de ce délai et, le cas échéant, être communiquées aux autorités policières ou judiciaires compétentes.

Pour finir, le responsable du traitement doit veiller à ce que les images soient détruites après l'écoulement du délai de conservation.

5. **L'article L. 261-1 nouveau du Code du travail :** les dispositions légales spécifiques concernant les traitements de données à des fins de surveillance dans le cadre des relations de travail

L'employeur qui souhaite installer une vidéosurveillance devra, **en plus du respect des points 1-4 ci-avant et des points 6-7 ci-après**, veiller au respect des **règles spécifiques de l'article L. 261-1 du Code du travail**.

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 modifie l'article L. 261-1 du Code de travail. Le législateur a ainsi fait usage de l'option laissée aux Etats membres par l'article 88 du RGPD de prévoir des modalités plus spécifiques concernant les traitements de données à caractère personnel de salariés dans le cadre des relations de travail.

La nouvelle version de l'article L. 261-1 du Code de travail autorise les traitements de données à caractère personnel à des fins de surveillance des salariés dans le cadre des relations de travail, par l'employeur, uniquement sur base d'**une des conditions de licéité limitativement énumérées** à l'article 6, point 1, lettres a) à f) du RGPD (voir point1.).

Pour pareils traitements de données à caractère personnel, dont la vidéosurveillance sur le lieu du travail, le nouvel article L. 261-1 du Code de travail prévoit tout d'abord une **obligation d'information collective préalable** à l'égard de la représentation du personnel, en plus de l'**information individuelle des salariés** découlant de l'article 13 du RGPD. Cette information **doit contenir** une description détaillée de la finalité du traitement envisagé, des modalités de mise en œuvre du système de surveillance, et le cas échéant, la durée ou les critères de conservation des données, de même qu'un engagement formel de l'employeur sur la non-utilisation des données collectées pour une finalité autre que celle prévue explicitement dans l'information préalable.

La nouvelle version de l'article L. 261-1 du Code de travail prévoit que, sauf lorsque la surveillance répond à une obligation légale ou règlementaire, la vidéosurveillance doit faire l'objet d'une **codécision entre l'employeur et la délégation du personnel (ou comité mixte)** et ce, conformément aux articles L. 211-8, L.414-9 et L. 423-1 du Code de travail, lorsqu'elle est mise en œuvre pour les finalités suivantes :

1. pour les besoins de sécurité et de santé des salariés, ou

2. pour le contrôle de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact, ou

3. dans le cadre d'une organisation de travail selon l'horaire mobile conformément au Code du travail.

Par ailleurs, dans tous les cas de projets de traitements de données à des fins de surveillance des salariés dans le cadre des relations de travail, la délégation du personnel, ou à défaut les salariés concernés, peuvent, dans les 15 jours suivant l'information préalable mentionnée ci-dessus, soumettre une **demande d'avis préalable** relative à la conformité du projet de traitement à la Commission nationale pour la protection des données, qui doit se prononcer dans le mois de la saisine. La demande a un effet suspensif pendant ce délai.

Enfin, la nouvelle version de l'article L. 261-1 du Code de travail rappelle que les salariés concernés ont toujours **le droit d'introduire une réclamation** auprès de la Commission

nationale en cas d'atteinte à leurs droits, une telle réclamation ne constituant ni un motif grave, ni un motif légitime de licenciement.

6. Faut-il effectuer une analyse d'impact relative à la protection des données (« AIPD ») en matière de vidéosurveillance ?

L'article 35 du RGPD requiert qu'une « AIPD » soit effectuée « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement,* ***est susceptible d'engendrer un risque élevé*** *pour les droits et libertés des personnes physiques* ».

Le paragraphe 3 de l'article 35 du RGPD prévoit en outre 3 cas dans lesquels une « AIPD » est particulièrement requise. L'un de ces 3 cas vise la « *surveillance systématique à grande échelle d'une zone accessible au public* ». Dans certaines situations, l'installation d'un système de vidéosurveillance pourrait tomber dans ce cas.

En outre, les « *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679* » émises par le groupe de travail européen (G29) précisent les 9 critères qu'il y a lieu de prendre en compte pour évaluer si un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, et donc, s'il faut ou non effectuer une « AIPD ». Certains de ces critères pourraient être remplis dans le cadre de la mise en place d'un système de vidéosurveillance, comme par exemple celui du traitement de « *données concernant des personnes vulnérables* » (salariés) et le critère de la « *surveillance systématique* ».

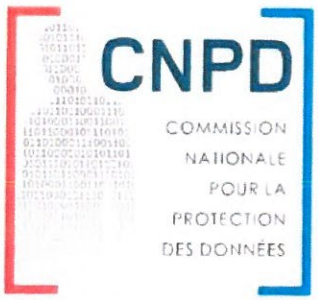
Le RGPD prévoit que les autorités de contrôle nationales établiront et publieront une liste des types d'opérations de traitement de données à caractère personnel pour lesquels une « AIPD » est requise. La CNPD adoptera prochainement cette liste, qui devra préalablement être communiquée, pour avis, au Comité européen de la protection des données.

7. Autres obligations à respecter en vertu du RGPD

En plus des principes énoncés dans les présentes lignes directrices, l'entièreté des dispositions du RGPD restent, bien entendu, applicables au traitement de données à caractère personnel que constitue la vidéosurveillance.

La CNPD souhaite attirer particulièrement l'attention des responsables du traitement sur l'obligation qui découle de l'article 32 du RGPD de mettre en place des **mesures techniques et organisationnelles** adéquates afin de garantir la sécurité et la confidentialité des données faisant l'objet d'un traitement.

En outre, la CNPD tient à rappeler que si un sous-traitant est impliqué (par exemple, une société de gardiennage) dans le traitement de données à caractère personnel résultant de la vidéosurveillance, un contrat de **sous-traitance** répondant aux critères de l'article 28 du RGPD devra être mis en place.



COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

1, avenue du Rock'n'roll I L-4361 Esch-sur-Alzette
Tél. : (+352) 26 10 60 - 1 I Fax. : (+352) 26 10 60 - 29

www.cnpd.lu

Avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique

Délibération n°36/2019 du 15 mars 2019

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n° 2016/680 du 27 avril 2016 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention 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 (ci-après désignée « la directive »), à laquelle se réfère l'article 8 de 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 (ci-après désignée « 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 Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD »), « conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données personnelles ».

Eu égard à la mission de conseil qui lui est attribuée, mais également de la tendance générale du renforcement de la surveillance des citoyens afin de pallier à l'insécurité et face aux préoccupations du public à ce sujet, la Commission nationale rend un avis circonstancié sur la création et l'exploitation par la Police grand-ducale d'un système de vidéosurveillance policière (ci-après désigné « VISUPOL ») au sein de zones de sécurités ciblées à Luxembourg-ville.

L'auto saisine de la CNPD intervient dans le cadre de l'abrogation de la base légale de VISUPOL suite à l'entrée en application de 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. En effet, celle-ci abroge l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, tel que modifié en 2007 (ci-après désignée « la loi du 2 août 2002 »). L'article en question fut le fondement légal de la création et de l'exploitation de VISUPOL. En application de l'article 17, un règlement grand-ducal du 1er août 2007 autorisait la création et l'exploitation de VISUPOL par la Police grand-ducale au sein de zones de sécurité (ci-après désigné « le règlement d'application »). Le règlement d'application déléguait la fixation des zones de sécurité concernées au ministre ayant dans ses attributions la Police grand-ducale à savoir, le Ministre de la Sécurité intérieure.

Les récentes modifications du cadre légal étant rappelées, la CNPD souhaite adopter une approche globale quant à l'utilisation de dispositifs de vidéosurveillance à des fins policières à savoir, la prévention, la recherche et la constatation des infractions[1]. Une telle approche

[1] Conformément à l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (abrogée) et l'article 2 de la loi du 18 juillet 2018 sur la Police grand-ducale et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; 3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ; 5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation :
1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. La loi du 23 juillet

nécessite de revenir sur les caractéristiques et les enjeux de la vidéosurveillance à des fins policières dans l'espace public (I), réflexion qui a pour objet de mettre en exergue l'importance de l'encadrement légal de la surveillance et du contrôle de l'espace public (II).

I. Les caractéristiques et les enjeux de la vidéosurveillance à des fins policières dans l'espace public

La vidéosurveillance policière, la captation d'images qui en émane et leurs utilisations ultérieures afin d'identifier les individus potentiellement dangereux ne sont pas de nouvelles méthodes. En effet, à la fin du XIXème siècle, le criminologue français Alphonse Bertillon, crée le premier laboratoire de police d'identification criminelle et l'anthropométrie judiciaire. Il développe des techniques de photographies uniformes et des méthodes de mesures du squelette humain afin d'identifier les criminels et les récidivistes[2].

De tous temps, les images du corps humains sont corrélées avec leurs comportements et présentées comme une solution miracle aux problèmes sociétaux[3]. Aujourd'hui encore, la vidéosurveillance est présentée comme le remède incontournable face à l'insécurité[4]. Néanmoins, les dispositifs de vidéosurveillance génèrent une surveillance et un contrôle social qu'il y a lieu de définir et d'analyser (A) afin de mesurer et de comprendre l'impact de tels dispositifs dans les droits et les libertés fondamentales reconnus aux individus (B).

A. Définir, comprendre, la surveillance et le contrôle social

Un cadre théorique qui s'imprègne de plusieurs disciplines telle que la sociologie et la philosophie, favorise la compréhension du fonctionnement de la surveillance et du contrôle mis en œuvre par un dispositif de vidéosurveillance policière tel que VISUPOL.

La sociologie tout d'abord, définit la surveillance comme étant « l'attention accrue portée à des personnes et des populations dans le but de les influencer, les gérer ou les contrôler »[5]. Les techniques de surveillance évoluent en fonction des évènements politiques, économiques et sociaux qui ponctuent et forgent la société. Le contrôle quant à lui, peut être défini comme l'action d'examiner ce qui est conforme ou ce qui ne l'est pas par rapport à une norme définie par le pouvoir. Il fait appel à la vérification du bon fonctionnement et de la qualité de la norme en question. La surveillance et le contrôle sont donc indissociables.

La philosophie quant à elle, favorise l'identification et la compréhension des caractéristiques de la surveillance et du contrôle. Michel Foucault dans son ouvrage *Surveiller et Punir. Naissance de la prison*[6] en identifie trois, à savoir : le découpage de l'espace (1), la surveillance hiérarchisée (2) et *in fine*, le savoir généré sur les individus (3).

1952 concernant l'organisation militaire ; 2. Le code d'instruction criminelle ; 3. La loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

[2] Pavlich, G, (2009), The subjects of criminal identification. Punishment & Society, 11 (2), p. 174 et suivantes. Voir également, Bertillon A., (1885), Identification anthropométrique. Instruction signalétique, Ministère de l'intérieur, Administration pénitentiaire, Melun, p. 132.

[3] Van der Walt J., (2015), « The Literary Exception : Reflections on Agamben's « Liberal Democratic » Political Theology and the Religious Destabilisation of the Political in our Time », in New perspectives. Interdisciplinary Journal of central & East European Politics and International Relations, 23 (1), p.17.

[4] Mucchielli L., *Vous êtes filmés !* Malakoff, Armand Colin, p. 228.

[5] Lyon, D. « Le 11 septembre, la "guerre au terrorisme" et la surveillance généralisée », in Bigo, D., Bonelli, L., & Deltombe, T. (2008), Au nom du 11 septembre. *Les démocraties à l'épreuve de l'antiterrorisme, Paris,* La Découverte, p. 93.

[6] Foucault, M. (1975). Surveiller et Punir. Naissance de la prison. Editions Gallimard, p. 360.

1) Le découpage de l'espace

L'identification des zones urbaines à surveiller est caractéristique de toutes stratégies de surveillance et de contrôle. Celle-ci y est généralement modulée en fonction des besoins de l'espace urbain et des risques qui y sont présents. A titre d'exemple, elle peut être plus intense dans une zone présentant un taux de criminalité élevé et peut être faible voire inexistante dans des quartiers résidentiels étant dénués de problèmes majeurs et n'ayant pas un degré d'activité élevé.

Les présentes considérations révèlent que la délimitation de ces zones se doit de répondre à des critères objectifs. A ce titre, le règlement d'application, pris en exécution de la loi du 2 août 2002, laquelle fût abrogée 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, , nous renseigne sur les objectifs de VISUPOL et des zones de sécurité mises en place. Elles ont pour objet la prévention, la recherche et la constatation d'infractions pénales[7]. Il révèle également que le découpage de l'espace n'est pas permanent. En effet, l'article 10 paragraphe 2 du même règlement précise que les zones de sécurité à surveiller sont désignées comme telles pour une durée de deux ans. Une fois ce délai expiré, la vidéosurveillance peut être prorogée suite à une évaluation de l'utilité et de la nécessité de celle-ci.

Au regard des nombreux règlements ministériels rendus ces dernières années, la CNPD constate que la Police grand-ducale effectue un découpage de l'espace en désignant des zones de sécurité à Luxembourg-ville. A cet égard, le règlement ministériel du 15 septembre 2017 portant désignation des zones de sécurités soumises à la vidéosurveillance de la Police grand-ducale révèle quels sont les espaces découpés. Il s'agit du quartier du Limpertsberg-Glacis (Zone A), du quartier de la Gare (Zone C) ainsi que les environs du stade « Josy Barthel » (Zone D). Le règlement ministériel du 28 mars 2018 portant prorogation de la vidéosurveillance dans la zone de sécurité « zone E » à Luxembourg-ville[8] quant à lui, renseigne sur l'existence d'une zone de sécurité supplémentaire dans le quartier du Kirchberg, autour du Centre de Conférence.

2) Une surveillance hiérarchisée

Toute stratégie de surveillance et de contrôle obéit à une hiérarchie stricte favorisant l'organisation et la bonne mise en œuvre de celle-ci. Il y a ceux qui conçoivent et ordonnent la mise en œuvre d'une telle stratégie, ceux qui s'occupent de la gestion et d'autres qui l'exécutent. La loi du 18 juillet 2018 sur la Police grand-ducale, en particulier son Chapitre 2 Section 1ère consacrée aux missions de police administrative ne donne aucune précision quant à la hiérarchie qui orchestre et exécute la vidéosurveillance des quartiers de Luxembourg-ville précédemment mentionnés. Le Chapitre 4 de ladite loi relatif aux relations de la Police avec d'autres autorités fait certes état dans sa section 1ère, des relations entre la Police grand-ducale et les autorités communales, telles que les bourgmestres[9]. La composition et la mise en œuvre

---

[7] 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. 1er.

[8] Ce règlement cessera d'être en vigueur le 28 mars 2019.

[9] Loi du 18 juillet 2018 sur la Police grand-ducale et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; 3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ; 5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation :
1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. La loi du 23 juillet

d'un comité de concertation régional[10] et d'un comité de prévention communal[11] y sont également mentionnés. Cependant, la CNPD constate qu'aucunes dispositions de ces articles ne sont consacrées aux acteurs impliqués dans le dispositif VISUPOL ne laissant pas entrevoir la hiérarchie qui orchestre ledit dispositif.

3) Générer un savoir sur les individus

Tout système de vidéosurveillance permet de générer un savoir conséquent sur les individus présents dans les zones de sécurité. L'attitude, la démarche, les activités et les déplacements des individus dans les lieux surveillés sont scrutés. Le regroupement de l'ensemble de ces éléments permet, dans une certaine mesure, de se faire une idée très précise sur les habitudes des individus surveillés et d'en générer un profil.

Cependant, la loi du 18 juillet 2018 sur la Police grand-ducale ne donne aucune indication relative au système VISUPOL si bien qu'il est impossible d'avoir des renseignements sur le type de savoir généré par le dispositif sur les individus. Des informations sont néanmoins données par l'article 3 du règlement d'application. Celui-ci dispose en effet que « le système de vidéosurveillance prend en image les zones de sécurité déterminées [...] et enregistre ces images sur un outil informatique ». Il est donc possible d'en déduire que VISUPOL se limite à la captation d'image.

B. L'impact de la société de surveillance et du contrôle social sur les droits fondamentaux et les libertés reconnues aux individus

Les droits fondamentaux et les libertés reconnus aux individus bénéficient d'une protection considérable à l'échelle européenne. En effet, la Convention européenne des droits de l'Homme (ci-après désignée « la CEDH »), en est la première illustration.
De surcroît, le traité de Lisbonne renforce la garantie des droits fondamentaux en érigeant la Charte des droits fondamentaux (ci-après désignée « la Charte »), au rang du droit primaire de l'Union européenne[12]. L'article 2 du traité sur l'Union européenne dispose que cette dernière est fondée sur des valeurs telles que le respect de la liberté et des droits de l'hommes. Les juges de la Cour de justice de l'Union européenne (ci-après désignée « CJUE) ainsi que de la Cour européenne des droits de l'Homme[13] (ci-après désignée « Cour EDH »), se portent également garant du respect des droits fondamentaux et des libertés.

L'objet de la présente partie est de mettre en exergue l'impact que les systèmes de vidéosurveillance peuvent avoir sur les droits fondamentaux. Le recours aux dispositifs de surveillance peut avoir pour effet de limiter le respect au droit à la vie privée et à la protection des données (1), il peut également être générateur de discrimination et de stigmatisation (2) et limite le droit à la libre circulation des individus au sein de l'espace public (3)[14].

1952 concernant l'organisation militaire ; 2. Le code d'instruction criminelle ; 3. La loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, articles 35 et 36.

[10] *Ibidem*, article 37.

[11] *Ibidem*, article 38.

[12] Article 6 paragraphe 1 du traité sur l'Union européenne, J.O.U.E., C 326, 26.10.2012, p. 13-390.

[13] La CNPD se focalisera davantage sur les arrêts rendus par la CJUE mais ce n'est pas pour autant qu'elle ignore les jugements rendus par la CEDH.

[14] La CNPD limite son analyse à ces trois droits fondamentaux mais cela ne veut pas dire que l'impact de la vidéosurveillance est limité à ces derniers.

1) La limitation du droit à la vie privée et à la protection des données par les dispositifs de vidéosurveillance

La vidéosurveillance au sein de l'espace public a pour effet de limiter le droit à la protection des données à caractère personnel protégé par la Charte[15] et dans une plus large mesure, le droit au respect de la vie privée et familiale protégé à la fois par la Charte[16] et la Convention européenne des droits de l'Homme[17] mais également par la Constitution Luxembourgeoise[18]. En effet, de tels dispositifs génèrent un savoir sur les individus, savoir qui a notamment fait l'objet de développements dans la jurisprudence de la CJUE et la Cour EDH.

A titre liminaire, la Commission nationale rappelle les propos de l'avocat général Villalon dans le cadre de l'arrêt de la CJUE *Digital Rights* qui affirme que ce savoir génère une « cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire un portrait complet et précis de son identité privée »[19]. La CNPD peut s'inspirer de cet arrêt de la CJUE et observer que les images émanant des dispositifs de vidéosurveillance « prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[20].

La Cour européenne des droits de l'homme quant à elle, considère également que le fait de surveiller les actes de personnes se trouvant dans un lieu public, notamment au moyen d'un système de vidéosurveillance, entraîne une ingérence dans la vie privée de ces personnes si le fait de surveiller est accompagnée d'un enregistrement et se fait de manière systématique ou permanente.[21]

La vidéosurveillance peut également avoir pour effet de générer de la discrimination et de la stigmatisation des individus se trouvant au sein des zones de sécurité.

2) La vidéosurveillance génératrice de discrimination et de stigmatisation

L'Union européenne est fondée sur des valeurs dont la non-discrimination fait partie[22]. L'interdiction de discrimination est également consacrée par la CEDH[23], la Charte[24] ainsi qu'au sein de la Constitution Luxembourgeoise[25].

A ce titre, la Commission nationale souhaite rappeler que les individus ne sont pas tous égaux face à la vidéosurveillance. En effet, le grand nombre de personnes se trouvant dans les zones surveillées et l'incalculable quantité d'images collectées sont autant de facteurs qui

---

[15] Article 8 de la Charte des droits fondamentaux de l'Union européenne, J.O.C.E., C 326 du 26.10.2012, p. 391.
[16] *Ibidem.*
[17] Article 8 de la Convention européenne des droits de l'Homme, signée à Rome, le 4.XI.1950.
[18] Article 11 (3), Constitution, Texte Coordonné à jour au 20 Octobre 2016, Recueil réalisé par le Ministère d'Etat – Service central de législation.
[19] Conclusion de l'avocat général Pedro Cruz Villalon dans les affaires jointes Digital Rights Ireland Seitlinger e.a., C-293/12 et C-594/12, EU :C :2013 :845, point 74.
[20] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point 27.
[21] Cour EHD, Peck c. Royaume-Uni, n° 44647/98, 28 janvier 2003, para.59.
[22] Traité sur l'Union européenne, J.O.U.E., C326, 26.10.2012, p. 13-390, article 2.
[23] Article 14.
[24] Article 21.
[25] Article 10 bis.

compliquent l'observation policière. Pour mener à bien sa mission, la police se doit donc d'effectuer une sélection des personnes à surveiller et des images collectées. Une distinction de ceux qui ont un comportement suspect et ceux qui en sont dénués s'opère.

De telles pratiques amènent la CNPD à s'interroger sur ce qu'est un comportement suspect et quels sont les critères permettant à la police d'identifier de tels comportements ?

Dans leur étude relative à l'impact de la vidéosurveillance, Prof. Norris et Prof. Armstrong révèlent que l'appartenance sociale, l'âge, l'ethnicité et le genre peuvent être des critères de sélection pris en compte par la police afin de cibler davantage l'observation des individus[26]. La démarche des individus, leurs styles vestimentaires, s'ils sont actifs, passifs, provoquants etc.,[27] sont autant d'éléments pris en compte lors de la surveillance. Leur étude révèle également que 36 % des personnes sujettes à une étroite observation le sont pour des « raisons évidentes », 24% des personnes sont surveillées à cause de leurs comportements et 34 % sur base de leur appartenance ethnique. Autres chiffres révélateurs : 65% des adolescents sont surveillés sans motifs particuliers, 68 % personnes de couleur ont fait l'objet d'une observation ciblée également sans motifs. Par conséquent, les jeunes, les personnes de couleurs et les hommes sont les personnes les plus surveillées sans motifs[28]. Ils concluent qu'une telle différenciation n'est pas basée sur des critères comportementaux et individuels objectifs mais fondée sur l'appartenance à un groupe social et par conséquent, ces pratiques sont discriminatoires pouvant accentuer la marginalisation et la stigmatisation des personnes ciblées[29] aboutissant à la mise en œuvre d'un tri social[30].

L'installation et l'utilisation de vidéosurveillance peut également avoir pour effet de limiter le droit à la libre circulation.

3) La limitation du droit à la libre circulation

La libre circulation des personnes est un droit fondamental de l'Union européenne. Il est consacré à l'article 2 du Protocole additionnel n°4 à la CEDH ainsi qu'à l'article 45 de la Charte des droits fondamentaux de l'Union européenne.

Il est indéniable que l'utilisation de vidéosurveillance dans les lieux publics limite la portée du droit à la libre circulation. En effet, les images émises par les dispositifs de vidéosurveillance peuvent avoir pour effet de suivre les individus, tracer leurs itinéraires quotidiens. Les individus peuvent avoir l'impression de ne pas être en mesure de circuler librement dans l'espace public sans faire l'objet d'un suivi constant[31].

L'étude des caractéristiques, des enjeux de la vidéosurveillance à des fins policières dans l'espace public étant faite et la nécessaire prise en considération du cadre légal actuellement en vigueur étant rappelée, il y a à présent lieu de souligner l'importance de l'encadrement légal de la surveillance et du contrôle qui prennent place au sein de l'espace public.

---

[26] Norris, C. and Armstrong, G., *The Maximum, Surveillance Society: The Rise of CCTV*, (1999 b), Oxford:Berg. Etude reprise *in* Lyon, D., *Surveillance as social sorting. Privacy, risk and digital discrimination*, Routledge, (2008), p. 266.
[27] *Ibidem.*
[28] *Ibidem.*
[29] *Ibidem.*
[30] Lyon D. (2003). *Surveillance as a social sorting: Privacy, risk, and digital discrimination*. Psychology Press, p.20.
[31] Groupe de travail "Article 29" sur la protection des données, Avis 4/2004 sur le traitement des données à caractère personnel au moyen de la vidéo-surveillance, adopté le 11 février 2004, 117/02/FR WP 89, disponible à la page : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp089_fr.pdf, consultée pour la dernière fois le 14/02/2019.

II. L'importance de l'encadrement légal de la surveillance et du contrôle de l'espace public

Doter d'une base légale un système de vidéosurveillance policière mis en œuvre au sein de l'espace public permet de poser des gardes fous quant à son utilisation et établir des garanties pour les personnes qui sont sujettes à la surveillance et au contrôle qui en émane. L'encadrement par un texte de loi d'un tel dispositif permet de freiner l'ubiquité de son installation et de ne pas considérer l'ensemble des individus comme des suspects potentiels.

L'objet de la présente partie est de mettre en exergue la manière dont le droit européen circonscrit l'ingérence faite dans les droits fondamentaux par des dispositifs de surveillance (A) et façonne le droit national en la matière (B).

A. L'encadrement de l'ingérence dans les droits fondamentaux occasionnées par des dispositifs de surveillance par le droit européen

L'impératif d'une base légale (1) et la qualité de la loi (2) sont des critères consacrés par le droit européen afin d'encadrer l'ingérence dans les droits fondamentaux émanent de stratégies de surveillance.

1) L'impératif de la base légale

La CNPD souhaite rappeler que le respect des droits fondamentaux n'est pas absolu puisqu'une ingérence dans ces derniers est reconnue à l'article 52 paragraphe 1 de la Charte. En effet, cet article dispose que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi »[32]. La CEDH quant à elle, rend également possible ladite limitation tout en la rattachant au respect de la vie privée et familiale par exemple[33].

La CJUE et la Cour EDH se sont prononcées à de nombreuses reprises sur la nécessité d'une loi encadrant l'atteinte qui est faite dans les droits fondamentaux. Dans l'arrêt *Digital Rights*[34] relatif à l'appréciation de la validité de la directive 2006/24/CE avec les articles 7 et 8 de la Charte ou encore dans l'avis 1/15 relatif à la conclusion de l'accord Passenger Name Record (PNR) entre l'Union européenne et le Canada[35], la CJUE a eu l'occasion de rappeler l'obligation de prévoir légalement toute ingérence dans les droits fondamentaux. La Cour EDH dans son arrêt *Kopp*[36] relatif à la mise sur écoute des lignes téléphoniques d'un cabinet d'avocats sur instruction du procureur général de la Confédération helvétique ainsi que dans l'arrêt *Amann*[37] relatif à l'interception d'une communication téléphonique, procède à la vérification de l'existence d'une base légale justifiant les limitations dans les droits fondamentaux, en particulier le droit au respect de la vie privée et familiale.

Emane de l'impératif que l'ingérence soit prévue par la loi, l'exigence de la qualité de celle-ci.

---

[32] *J.O.U.E.*, C 326, 26.10.2012, p.391-407.
[33] Article 8 paragraphe 2 de la Convention européenne des droits de l'Homme, signée à Rome, le 4.XI.1950.
[34] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point 38.
[35] Avis 1/15, du 8 septembre 2016, EU :C :2016 :656.
[36] Cour EDH, Kopp c. Suisse, n° 23224/94, 25 mars 1998, para. 56 à 61.
[37] Cour EDH, Amann c. Suisse [GC], n° 27798/95, 16 février 2000, para. 46 à 54.

2) La qualité de la loi

La qualité de la loi, en particulier en matière pénale, s'apprécie au regard du respect du principe de légalité des incriminations. En effet, la légalité des peines est l'énonciation dans la loi des comportements incriminés[38]. Elle a pour effet d' « assurer la meilleure connaissance possible de la loi pénale ; favoriser la prévisibilité et sécurité dans les échanges sociaux[39] », garantir le principe de la hiérarchie ; de séparation des pouvoirs et par là, limiter l'arbitraire du juge. A l'échelle supra nationale, ce principe est consacré par la CEDH à son article 7 qui le perçoit comme un droit absolu auquel nul ne peut déroger[40]. Par conséquent, celui-ci appartient aux principes généraux du droit de l'Union européenne[41].

Du principe de légalité émane la prévisibilité de la loi, principe selon lequel un individu suffisamment informé doit savoir quels sont les comportements pouvant faire l'objet d'une surveillance dans l'espace public.

Ainsi, conformément au principe de légalité de la loi pénale, la CNPD affirme que les individus doivent pouvoir être tenus informés sur les comportements qui attirent particulièrement l'attention des agents de la Police grand-ducale lors de visionnage des images.

La Cour EDH et la CJUE rappellent également quels sont les critères que la loi doit remplir pour faire preuve de qualité.

La Cour EDH affirme que « les mots « prévue par la loi » impliquent des conditions qui vont au-delà de l'existence d'une base légale en droit interne et exigent que celle-ci soit « accessible » et « prévisible » »[42]. Elle ajoute que ces termes impliquent que « le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par l'article 8 paragraphe 1 »[43]. Par conséquent, la loi « doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire »[44].

La CJUE quant à elle, rappelle l'importance « de prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »[45].

---

[38] Beccaria, C., (1870). Des délits et des peines. Guillaumin.

[39] Cartuyvels Y., "Les paradigmes du droit penal moderne en période "postmoderne": évolutions et transformations, *in* Massé M., J-P. Jean, Giudicelli A. (sous la dir), (2009). Un droit pénal postmoderne ? Mise en perspective des évolutions et ruptures contemporaines. Presses universitaires de France, p. 77.

[40] Cartuyvels Y., Guillain C., Kerchove M., Tulkens F. (Ed.), (2010), *Introduction au droit pénal. Aspects juridiques et criminologiques,* Bruxelles, Kluwer, p. 225.

[41] Traité sur l'Union européenne, J.O.U.E., C 326, 26.10.2012, p. 13-390, article 6 paragraphe 3.

[42] Cour EDH, Amann c. Suisse [GC], n° 27798/95, 16 février 2000, para, 55.

[43] *Ibidem*, para 56.

[44] *Ibidem*. Voir également Cour EDH, Malone c. Royaume-Uni, série A n°82, du 2 août 1984, pp. 31-32, para.66 ; Cour EDH, Fernández Martínez c. Espagne CE:ECHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, Liberty et autres c. Royaume-Uni, n° 58243/00, du 1er juillet 2008, para. 62 et 63; Cour EDH, Rotaru c. Roumanie, App. N° 28341/95, 4 mai 2000, para. 57 à 59 et Cour EDH, S et Marper c. Royaume-Uni, Requêtes n° 30562/04 et 30566/04, du 4 décembre 2008 para. 99.

[45] Arrêt du 6 octobre 2015, Schrems, C-362/14, EU :C :2015 :650, point 91. Voir également en ce sens Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point, 54,

L'encadrement de l'ingérence dans les droits fondamentaux et les libertés étant effectué par le droit européen, il y a à présent lieu d'analyser la mise en œuvre d'un tel encadrement à l'échelle nationale.

B. La limitation de l'exercice des droits fondamentaux par le droit national

Compte tenu de l'obligation imposée par le droit européen et au regard de la jurisprudence de la CJUE et la Cour EDH, la CNPD estime qu'en principe, les Etats membres n'ont pas d'autres choix que de prévoir une base légale pour toute limitation à l'exercice des droits fondamentaux et des libertés. L'installation de systèmes de vidéosurveillance à des fins policières ne fait pas exception à la règle. De nombreux pays européens ayant recours à la vidéosurveillance dans l'espace public dote cette dernière de base légale, c'est le cas de nos pays voisins, la France (1), la Belgique (2) et l'Allemagne (3).

1) L'exemple français

En France, le nombre de caméras filmant l'espace public a fortement augmenté pour lutter contre l'insécurité[46]. L'installation de systèmes dits de vidéo protection est prévue par le Code de la sécurité intérieure[47]. Les objectifs de l'installation de tels dispositifs au sein de l'espace public y sont prévus. Il s'agit notamment de prévenir les atteintes à la sécurité des personnes et des biens dans des zones déterminées[48], de prévenir des actes de terrorisme[49], des risques naturels ou technologiques etc.[50]. En ce qui concerne leurs autorisations, celles-ci sont données par le préfet[51] pour une durée de cinq ans renouvelable[52]. Le Code de la sécurité intérieure fait également mention des personnes en charge du visionnage des images[53], celles et ceux pouvant avoir accès à ces dernières[54] ainsi que la durée de conservation des images qui ne peut excéder un mois[55]. De surcroit, les autorités en charge de la gestion et de l'évaluation des dispositifs de vidéo protection telles que les Commissions départementales[56] et nationale[57] de la vidéo protection et la Commission nationale de l'informatique et des libertés[58] y sont également précisées.

Le présent développement révèle que la France a doté d'une base légale l'installation et la mise en œuvre des caméras de surveillance au sein de l'espace public. Celle-ci répond aux critères de qualité de la loi consacrés par le droit européen et la jurisprudence de la Cour EDH et de la CJUE.

---

[46] Mucchielli L., *Vous êtes filmés !* Malakoff, Armand Colin, p. 25 et suivantes.
[47] Titre V du Code de la sécurité intérieure.
[48] *Ibidem*, article L251-2, 5°.
[49] *Ibidem*, articles L251-2, 6° et articles L223-1 et suivants.
[50] *Ibidem*, article L251-2.
[51] *Ibidem*, article L252-1.
[52] *Ibidem*, article L252-2
[53] *Ibidem*, article L252-2.
[54] *Ibidem*, article L252-3.
[55] *Ibidem*, article L252-5.
[56] *Ibidem*, articles L251-4 ; L253-1.
[57] *Ibidem*, articles L251-5, 6 et 7.
[58] *Ibidem*, articles L251- 4 et ; L253-2, 3, 4 et 5.

2) L'exemple belge

En Belgique, la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police[59] est la base légale encadrant la vidéosurveillance dans l'espace public à des fins policières. Cette loi intervient dans un contexte de lutte anti-terroriste et anticipe l'entrée en application du RGPD et de la directive. Celle-ci prévoit en effet les conditions dans lesquelles les services de police peuvent avoir recours au dispositif de vidéosurveillance[60]. La loi précise également que l'utilisation d'un tel dispositif s'effectue sur décision et sous la responsabilité du fonctionnaire de police qui est également tenu de veiller au respect des principes de proportionnalité et de subsidiarité[61]. Tout comme la loi française, la législation belge prévoit une autorité en charge de l'évaluation des dispositifs de vidéosurveillance. En effet, il s'agit du Conseil Communal de la commune concernée par l'installation de ces derniers ou du ministre de l'Intérieur (ou de son délégué), concernant les services de police fédérale[62].
De surcroît, la durée de conservation n'excédant pas douze mois des données à caractère personnel collectées par les caméras[63], ainsi que l'accès aux images pour des finalités judiciaires et autres, sont prévus[64].

Il ressort du présent développement que les dispositifs de vidéosurveillance au sein de l'espace public à des fins policières est prévu légalement en droit belge. Il en est de même en droit allemand.

3) L'exemple allemand

La loi fondamentale pour la République fédérale d'Allemagne protège entre autres, la dignité de l'être humain et le caractère obligatoire des droits fondamentaux pour la puissance publique[65], la liberté d'agir, l'égalité devant la loi[66] ou encore la liberté de circulation et d'établissement[67]. De surcroît, la loi fondamentale prévoit que la restriction d'un droit fondamental doit être prévu par la loi[68].

La Cour constitutionnelle allemande veille au respect de l'article 19 de la loi fondamentale puisqu'elle consacre l'exigence d'une base légale pour la vidéosurveillance des espaces publics. Elle s'est aussi préoccupée de la surveillance des comportements des personnes concernées qui représente selon elle une atteinte aux droits fondamentaux. Le caractère attentatoire aux droits fondamentaux ne disparaît ni par le fait que la vidéosurveillance ait lieu dans l'espace public (et non en des lieux privés), ni par l'information des personnes concernées, ni par l'absence de contestations de la part de celles-ci[69]. La Cour

---

[59] modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière.
[60] *Ibidem*, article 8.
[61] *Ibidem*, article 10.
[62] *Ibidem*, article 9.1.
[63] *Ibidem*, article 11.
[64] *Ibidem*, article 12.
[65] Deutscher Bunderstag, Loi fondamentale pour la République fédérale d'Allemagne, article 1, La loi est disponible à l'adresse : https://www.bundestag.de/resource/blob/189762/f0568757877611b2e434039d29a1a822/loi_fondamentale-data.pdf, consultée pour la dernière fois le 14/03/2019.
[66] *Ibidem*, article 18.
[67] *Ibidem*, article 11.
[68] *Ibidem*, article 19.
[69] Bundesverfassungsgericht, Beschluss vom 23. Februar 2007 - 1 BvR 2368/06, points 38 à 40, disponible à la page :

constitutionnelle en déduit que la mise en place d'une vidéosurveillance nécessite une base légale qui doit respecter les principes de clarté et proportionnalité.[70] L'absence d'une telle législation a pour conséquence de soumettre les citoyens à l'arbitraire des autorités[71]. La Cour précise également que le degré de précision de la loi requis est déterminé en fonction de l'intensité de l'atteinte aux droits fondamentaux, et, pour ce qui est de la vidéosurveillance d'un lieu public, l'atteinte est jugée particulièrement importante puisqu'il s'agit d'une mesure visant indistinctement toutes les personnes se trouvant sur les lieux faisant l'objet d'une vidéosurveillance et que la plupart des personnes concernées n'ont rien à se reprocher[72].

C'est aux Länder que revient la responsabilité de légiférer en matière de vidéosurveillance au sein de l'espace public. A ce titre, la Rhénanie-du-Nord-Westphalie[73] et Hambourg[74] peuvent être pris pour exemple[75]. Ces législations déterminent les critères en fonction desquels les caméras sont installées, les personnes et institutions décidant de la mise en place des caméras et la durée de conservation des images.

Pour ce qui est des critères déterminant les lieux d'installation des caméras, il y a lieu, selon ces législations, de tenir compte des infractions ayant été commises dans le passé et ce celles probables dans le futur.

La législation du Land de Rhénanie-du-Nord-Westphalie précise par ailleurs que la vidéosurveillance ne peut être mise en œuvre que s'il est assuré que la Police peut intervenir très rapidement en cas d'infraction. En effet, une vidéosurveillance d'un côté sans garantie d'une intervention rapide de l'autre est jugée inadmissible pour l'Etat de droit.[76]

Ainsi, tout comme ses voisins français et belge, l'Allemagne encadre légalement l'installation et la mise en œuvre de la vidéosurveillance au sein de l'espace public et respecte le droit européen et la jurisprudence des juridictions européennes à cet égard.

Conclusion

L'étude des caractéristiques et des enjeux de la vidéosurveillance à des fins policières dans l'espace public, la surveillance, le contrôle social qui en émanent et l'impact de tels dispositifs dans les droits fondamentaux et les libertés reconnues aux individus, sont autant de raisons qui justifient l'importance de l'encadrement légal des dispositifs tels que VISUPOL.

En effet, la CNPD 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

---

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2007/02/rk20070223_1bvr236806.html, consultée pour la dernière fois le 13/03/2019.

[70] *Ibidem*, point 41.

[71] *Ibidem*, point 46.

[72] *Ibidem*, points 51 et 52.

[73] § 15a Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW), disponible à la page: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=1&bes_id=5173&anw_nr=2&aufgehoben=N&det_id=423939, consultée pour la dernière fois le 13/03/2019.

[74] § 8 Abs. 3 PolDVG (Gesetz über die Datenverarbeitung der Polizei), disponible à la page: http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-PolDVGHArahmen&doc.part=X&doc.origin=bs, consultée pour la dernière fois le 13/03/2019.

[76] Voir à ce sujet les travaux parlementaires de la législation du Land de Rhénanie-du-Nord-Westphalie p.10disponibles à la page : https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD17-3865.pdf,consultée pour la dernière fois le 13/03/2019.

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.

Néanmoins, la Commission nationale souhaite rappeler que de telles limitations sont possibles à condition d'être légalement prévues. L'existence d'un tel impératif s'explique notamment par le fait que les personnes dont les droits fondamentaux et les libertés sont limités doivent disposer de garanties suffisantes permettant de se protéger efficacement contre les risques d'abus à leur encontre[77].

La base légale est également utile aux législateurs et aux juges dans l'appréciation de la nécessité et du caractère proportionné de la mesure qui sont des conditions parmi d'autres que les ingérences doivent remplir[78]. Par conséquent, elle permet de s'assurer que l'installation et l'utilisation de la vidéosurveillance à des fins policières répond à des critères objectifs tel que la lutte contre la délinquance et non subjectifs tel que le sentiment d'insécurité ressenti par les individus.

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.

Dans ce contexte, la CNPD salue la déclaration récente du Ministre de la Sécurité intérieure qui considère « *qu'il est opportun de réfléchir à la mise en place d'un cadre légal spécifique pour l'installation future de caméras de surveillance* »[79]. Cette prise de position concorde d'ailleurs avec la volonté du gouvernement de vouloir légiférer pour ce qui est de l'utilisation projetée des « bodycams » par la Police grand-ducale si l'on se réfère à l'accord de coalition du gouvernement qui précise que : « *L'expérience pratique visant l'introduction des caméras portées sur le corps et, le cas échéant, de caméras embarquées dans les véhicules sera menée. Un cadre légal précis et applicable en matière d'enregistrement des données à caractère personnel lors des interventions policières devra être établi* ». Les présentes suggestions de la Commission nationale se font également l'écho des principes de légalité et de qualité de la loi, consacrés par le droit européen et la jurisprudence de la Cour de Justice de l'Union Européenne et la Cour Européenne des Droits de l'Homme.

La CNPD souhaite ajouter que le présent avis n'est pas limité au dispositif VISUPOL de la Police grand-ducale qui, pour l'instant n'est opérée que sur le seul territoire de la Ville de Luxembourg. En effet, dans la mesure où les responsables de certaines communes ont aussi manifesté leur intention de vouloir surveiller des espaces et lieux publics situés sur leurs territoires communaux, le présent avis a une portée générale qui a vocation à couvrir tout dispositif de vidéosurveillance, ayant une finalité de sécurité publique, peu importe qu'il soit opéré au niveau national par la Police grand-ducale ou au niveau local par des communes.
Ainsi, quel que soit le choix de base légale, celle-ci aura pour effet de mettre en exergue qu'au sein d'une démocratie telle que le Luxembourg, un des pays fondateurs de l'Union européenne

---

[77] *Ibidem*, point 54.
[78] Article 52 paragraphe 1 de la Charte des droits fondamentaux d l'Union européenne, J.O.U.E., C 326, 26.10.2012, p.391-407.
[79] Communiqué par le ministère de la Sécurité intérieure du 12/03/2019, disponible à la page : https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/03-mars/12-bausch-videoprotection.html, consultée pour la dernière fois le 12/03/2019.

et protecteurs de ses valeurs[80], la Police grand-ducale ou encore les communes, exercent leurs missions de surveillance résultant d'une interaction complexe entre des règles juridiques, organisationnelles, professionnelles, situationnelles et interactionnelles[81].

Ainsi décidé à Esch-sur-Alzette en date du 15 mars 2019.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Christophe Buschmann
Commissaire

[80] Article 2 du Traité sur l'Union européenne,
[81] Lyon D., Surveillance as social sorting: Privacy, risk, and digital discrimination, Routledge, 2003, p.252