Livre Blanc

Vidéoprotection

Mieux comprendre le cadre règlementaire
et les réalités d'installation et d'usage

GPMSE
Groupement Professionnel
des Métiers de la Sécurité Électronique

Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

TKH GROUP
AASSET security
TKH SECURITY SOLUTIONS

Sommaire analytique

REMERCIEMENTS

Ce livre blanc est l'aboutissement d'une concertation et d'un travail commencé en avril 2013 à l'initiative de Maître Alain Bensoussan, Virginie Cadieu (AASSET-SECURITY INTERNATIONAL - TKH SECURITE FRANCE) et Michel George (*GPMSE*).

Merci aux différents acteurs, qu'ils soient donneurs d'ordre du secteur public et privé, représentants d'organismes professionnels, dirigeants de cabinets de Conseils, présidents d'association ou de syndicats… qui ont permis d'apporter un regard multisectoriel et pluridisciplinaire sur d'importants enjeux, rencontrés au quotidien, dans le domaine de la vidéoprotection.

Merci plus particulièrement pour leur temps et la qualité de leur collaboration à

Mesdames
Emmanuelle Kawala**,** *Responsable du droit d'accès PP-DOSTL SDSIC MIVAP*
Isabelle Pottier, avocat ALAIN BENSOUSSAN - AVOCATS
Elisabeth Sellos-Cartel, *Adjointe au Préfet délégué aux coopérations de sécurité spécifiquement en charge des questions liées au développement de la vidéoprotection- Ministère Intérieur*
Christine Terracol, *Direction de la Sûreté - Département Défense- SNCF*
Stéphanie Tucoulet, *Secrétaire générale - SVDI*
Fabienne Villars, *Correspondant informatique et libertés - RENAULT*

Messieurs
Philippe Abbas*, Chef de produits vidéoprotection - DELTA SECURITY SOLUTIONS*
Frédéric Benoît, *Directeur de la Police Municipale de Montgeron*
Jean-Charles Bentata*, Directeur du CSU de la CAVAM*
Olivier Chadeau, *Responsable du pôle juridique – Inter Mutuelles Téléassistance*
Philippe Combey, *Directeur - IP Sécurité Conseils*
Garry Goldenberg*, Président d'Open IPVidéo*
André Molinengo*, Responsable du Centre de Réception des Alarmes - SOCIETE GENERALE*
Gilles Robine, *Chef de la MIVAP - Préfecture de police de Paris*
Jacques Tabard*, Responsable coordination sécurité réseau France - RENAULT*
Emmanuel Walle, avocat ALAIN BENSOUSSAN - AVOCATS

qui ont partagé leurs expériences et connaissances, durant plus d'une année, de façon très active et ont fournis la matière première à la synthèse que nous avons tenté de rédiger.

Merci également à toutes celles et ceux qui ont ponctuellement participé, notamment par leurs remarques et en nous aidant à rassembler les indispensables informations.

Ce livre blanc a pour vocation d'apporter des éclaircissements, mais aussi à susciter des réflexions.

En libre accès et gratuit sur les sites Aasset-Security international, GPMSE, ALAIN BENSOUSSAN – AVOCATS, SVDI, il pourra être amené à être complété et étoffé, après sa présentation au salon Expoprotection le 4 novembre 2014.

1. Pourquoi ce livre blanc ?

1.1 Génèse du projet

1. Le régime juridique de la vidéoprotection a été modifié depuis la Loppsi 2 : nouvelle terminologie, extension des possibilités d'y recourir, nouveaux types de contrôles, nouvelles garanties, nouvelles responsabilité, etc.

2. Les membres du GPMSE, les équipes du groupe AASSET Sécurity et du Cabinet Alain Bensoussan souhaitent apporter un regard multisectoriel et pluridisciplinaire sur ces problématiques à travers la rédaction d'un livre blanc.

3. Ce Livre Blanc s'adresse à tous ceux qui veulent prendre la mesure des responsabilités liées à la vidéoprotection, et qui, au-delà des seuls aspects techniques, veulent aussi prendre en compte les aspects juridiques associés.

4. Par la diffusion de ce Livre Blanc, nous souhaitons participer à une meilleure compréhension par tout un chacun des réalités de la vidéoprotection et faire en sorte que la « sécurité » reste le maître mot des utilisateurs.

5. Son objectif est de faciliter le travail des acteurs du marché de la vidéoprotection et des utilisateurs à chacun de leur niveau d'implication (dirigeants, collaborateurs et service informatique gérant les dispositifs de vidéoprotection, prestataires), tout en permettant un dialogue entre ces diverses populations autour de ce sujet.

6. Il est le fruit de l'expérience réunie de l'ensemble des membres du groupe de travail, acteurs de la vidéoprotection, contributeurs bénévoles aux profils variés (ingénieurs, responsables techniques, directeurs de CSU, juristes, etc.), et résulte d'une collaboration active de plusieurs mois.

7. Ce Livre Blanc parait particulièrement opportun à l'approche de la réforme de la loi de 1983, texte fondateur pour le secteur de la sécurité privée.

1.2 Avant-propos

8. Ce groupe a été constitué en avril 2013 en vue de mener une réflexion sur les principales problématiques liées aux activités de vidéoprotection.

9. Les premières réunions ont eu pour objectif de recenser :

- les questions et les incertitudes des professionnels de la sécurité et utilisateurs de dispositifs ;
- les textes permettant de compléter le référencement légal et la jurisprudence associée en la matière.

10. Les questions soulevées ont été très nombreuses :

- les différentes règles applicables (autorisation, déclaration, agrément, certification, etc.)
- la double déclaration "préfecture / Cnil" et le périmètre de la responsabilité ;
- le rôle respectif de tous les intervenants de la vidéoprotection (préfectures, commissions départementales, CNV, Cnil, comités d'entreprises, collectivités locales, bailleurs sociaux, installateurs, responsables sécurité, etc.) ;
- les précautions à prendre lors de l'installation d'un dispositif de vidéoprotection ;

- le rôle des CSU communaux et la possibilité de mutualiser des images avec les services de police ;
- le masquage des zones privées
- les personnes habilitées à visionner les images enregistrées et le statut des vidéo opérateurs ;
- les caméras vidéo mobiles (systèmes embarqués, drones, etc.) ;
- la durée de conservation des images ;
- le droit d'accès aux images ;
- le caractère obsolète de l'arrêté technique du 3 août 2007 ;
- les outils appropriés pour mieux relayer l'information auprès des entreprises (charte d'éthique, guide d'installation, formations, etc.) ;
- …

11. Ce livre blanc a pour vocation de tenter d'apporter des réponses :

- Pour une meilleure connaissance du droit et des fondamentaux de la sécurité (sécurité = droit fondamental - droit de la sécurité et droit à la tranquillité… Des notions différentes - cas des bailleurs sociaux, par ex.)

- Concernant certains flous ou désaccords au sujet des déclarations à réaliser, lors de la mise en place de certains dispositifs de vidéoprotection (quelles délimitations exactes - CNIL ou préfectures) - délimitations des périmètres à identifier.

- Relatives aux finalités de la mise en place de dispositifs de vidéoprotection (protection/prévention/surveillance ? à l'égard des propres salariés ? Quelles limites, au regard de la loi ? quels pouvoirs de la CNIL lors de contrôles ?)

- Au sujet des éventuelles obligations de conseils et/ou informations émanant des professionnels du secteur (Quelles responsabilités, Quels acteurs, Quelles limites ?)

- Concernant la place de la technologie dans l'évolution réglementaire

- La (les) sécurisation(s) ? au niveau des procédures de consultation des images, mais aussi au niveau des réseaux (recommandations ANSSI)

- Le droit d'accès aux images (personne - motivations – mise en œuvre pratique - refus)

- Quid des évaluations - missions de contrôles

- La réforme du livre VI du Code de la sécurité intérieure (ancienne loi de 1983)

1.3 Thèmes de l'étude

12. Un premier bilan de la synthèse des nombreuses problématiques soulevées par les membres du groupe de travail vidéoprotection a permis d'orienter les travaux sur quatre thématiques qui se sont transformées en trois thématiques au fur et à mesure de l'avancement des travaux, au sein de trois sous-groupes de travail.

- Sous-groupe : Le droit d'accès aux images

- Sous-groupe : Mobilité, interopérabilité, mutualisation des images et partage des compétences (CSU/PC sécurité)

- Sous-groupe : Le statut des vidéo opérateurs (vidéo surveillants) de CSU (Centre de supervision urbain)

13. Outre ces thématiques, le Livre Blanc rappelle en première partie, les fondamentaux techniques de la vidéoprotection et contient un glossaire des principaux termes du domaine (Annexe 7.1).

14. Il ne traite pas des besoins de la refonte de l'arrêté technique du 3 août 2007, qui ont fait l'objet d'un Livre blanc produit par L'Association nationale de la vidéoprotection (AN2V) en février 2014[1] et auquel nous renvoyons.

1.4 Avertissement

15. Le présent Livre blanc a pour unique vocation d'être un cercle de réflexion autour des activités de la vidéoprotection et non de préconiser des solutions dans la mise en œuvre de dispositifs de vidéoprotection.

16. Ce Livre blanc ne peut aucunement se substituer aux conseils avisés de spécialistes techniques ou juridiques de la sécurité des systèmes d'information.

2. Rappels des fondamentaux réglementaires de la vidéoprotection

17. Actuellement, les règles relatives à l'installation d'un dispositif de vidéoprotection relèvent de textes spécifiques, selon le lieu d'implantation du dispositif mis en place :

- dans les lieux non ouverts au public (locaux d'entreprise, habitation), les dispositifs sont soumis aux dispositions de la loi du 6 janvier 1978 modifiée dès lors que les images sont enregistrées et conservées dans des traitements informatisés ;

- sur la voie publique et dans les lieux ouverts au public, les dispositifs sont soumis aux dispositions du Code de la sécurité intérieure (ancienne Loi du 21 janvier 1995 codifiée) ;

18. Mais l'installation de tels dispositifs relève également de différentes législations qui ne sont pas propres à la vidéoprotection :

- la protection de la vie privée tel qu'en disposent l'article 9 du Code civil et l'article 226-1 du Code pénal.

- le droit du travail à travers l'information et la consultation des instances représentatives du personnel s'agissant des conditions de travail, de la surveillance et du contrôle des salariés (C. trav. articles L1121-1, L1221-9, L1222-4, L2323-32, L 4612-8 et s.)[2].

2.1 La notion de lieux ouverts au public

19. La circulaire du 14 septembre 2011 apporte une précision sur les compétences respectives de la Cnil et des Commissions de vidéoprotection. Selon celle-ci, appelée circulaire « relative au cadre juridique applicable à l'installation de caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre part »[3] :

[1] Livre blanc AN2V – 13 Février 2014, http://www.an2v-pixel.com/
[2] Voir la fiche pratique Cnil, La vidéosurveillance sur les lieux de travail, janvier 2013.
[3] Circulaire du 14 septembre 2011 : JO du 15 septembre 2011.

« Constituent des lieux ouverts au public les lieux dont l'accès est libre (plages, jardins publics, promenades publiques, commerces, etc.) ainsi que les lieux dont l'accès est possible, même sous condition, dans la mesure où toute personne qui le souhaite peut remplir cette condition (paiement d'un droit d'entrée, par exemple au cinéma) ».

20. Ces notions ainsi que leur cadre juridique seront par ailleurs développées aux pages suivantes.

21. Aux termes de cette même circulaire :

« Sont considérés comme des lieux non ouverts au public, les parties communes des immeubles d'habitation, les locaux professionnels et les établissements affectés à l'enseignement ou à la garde d'enfants ».

22. Pour la jurisprudence, un lieu public « est un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions ».

23. Le simple paiement d'une somme d'argent n'est pas considéré comme constituant une restriction d'accès. Ainsi les commerces, les cinémas, les restaurants, les services publics recevant des usagers, les parcs d'attraction sont considérés comme des lieux ouverts au public.

24. Ont notamment été considérés comme des lieux privés :

- l'intérieur d'une propriété privée[4] ;
- les parties communes d'une copropriété, notamment un parking souterrain et le garage constituant une annexe du domicile[5] ;
- la salle des délibérés d'une cour d'assises[6] ;
- l'intérieur d'un véhicule automobile circulant sur la voie publique[7].

25. Les parties communes d'une copropriété, notamment un parking souterrain, un hall d'immeuble, un garage annexe du domicile, l'intérieur d'un véhicule, un locaux d'entreprise ne recevant pas de public constituent un lieu privé.

26. A contrario, un lieu public est un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions.

27. La jurisprudence considère que les lieux ouverts au public redeviennent des lieux privés en dehors de leurs heures d'ouverture[8].

2.2 La notion de traitement de données à caractère personnel

28. Aux termes de l'article 2 de la loi du 6 janvier 1978 modifiée :

- « Constitue une **donnée à caractère personnel** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

[4] Cass. crim. 14 janvier 2014, pourvoi n°13-84909
[5] Cass. crim. 27 novembre 2013 pourvoi n°13-85042
[6] Cass. crim., 16 février 2010, pourvoi n°09-81492
[7] Cass. crim., 12 avril 2005, pourvoi n° 04-85637.
[8] Cass. crim. 14 mars 1984, pourvoi: n°83-90029, à propos d'un local commercial.

-

- « Constitue un **traitement de données à caractère personnel** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

-

- « Constitue un **fichier de données à caractère personnel** tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés ».

29. Comme le précise le Conseil d'Etat dans un avis du 24 mai 2011[9], « (…) la surveillance exercée en certains lieux au moyen de caméra doit être regardée comme un traitement automatisé de données à caractère personnel, entrant dans le champ de la directive du 24 octobre 1995 et de la loi du 6 janvier 1978, dès lors, d'une part, que les images font l'objet d'un enregistrement et d'une conservation et, d'autre part, que le responsable du système de surveillance ou ceux qui ont vocation à accéder aux enregistrements sont en mesure d'identifier les personnes qui y apparaissent ».

30. Il convient donc que les deux critères soient réunis.

31. Pour le Conseil d'Etat, « Le fait d'enregistrer, conserver puis, le cas échéant, effacer les images captées par la caméra est constitutif d'un traitement au sens (…) de l'article 2 de la loi. Ces opérations étant réalisées au moyen d'un dispositif automatique, le système de surveillance doit être regardé, quelles que soient les techniques mises, en œuvre, comme un traitement automatisé » [10].

32. En revanche, il considère que « le seul fait de capter les images au moyen d'une caméra et de les visionner en temps réel sans procéder à un enregistrement n'implique pas un traitement de données et n'entre donc pas dans le champ de la directive ni de la loi » [11].

2.3 Systèmes de vidéoprotection relevant du Code de la sécurité intérieure

2.3.1 L'autorisation préfectorale

33. Les dispositifs de vidéoprotection installés sur la voie publique et dans les lieux ouverts au public sont soumis aux dispositions du Code de la sécurité intérieure.

34. Ces dispositifs doivent obtenir une autorisation du préfet du lieu d'implantation, après avis d'une commission départementale présidée par un magistrat[12].

35. Leur installation est limitée par un cadre juridique qui garantit un droit d'information, d'accès et de recours aux particuliers[13].

36. La demande d'autorisation est encadrée par les articles R251-1 à R253-4 du Code de la sécurité intérieure.

37. Elle s'effectue au moyen des formulaires cerfa n°13806-03 et cerfa n°14095-02 (pour un établissement bancaire)[14].

[9] CE Avis n° 385.125 (section de l'intérieur) du 24 mai 2011.
[10] CE Avis n° 385.125 précité.
[11] CE Avis n° 385.125 précité.
[12] CSI, art. L252-1 à L252-7.
[13] CSI, art. L223-1 à L223-9.

38. Lorsque le demandeur remplit le formulaire Cerfa en indiquant qu'il a choisi un installateur certifié, il ne peut le faire que si la certification est réelle. L'indication dans le formulaire Cerfa du nom de l'installateur et de son numéro de certification constitue une information certaine.

39. Si après avoir adressé sa demande en indiquant que l'installation sera réalisée par un installateur certifié, un problème survient modifiant cette situation (recours à une société de sous-traitante non certifiée), il est nécessaire de le préciser en adressant à la préfecture une demande de modification accompagnée de l'attestation de conformité. En cas de maintenance, il sera également nécessaire de modifier les informations relatives aux personnes habilitées à accéder aux images.

40. L'autorisation est délivrée pour une durée de 5 ans renouvelable.

41. Le défaut d'autorisation fait l'objet de sanction (Code pénal, article L254-1).

2.3.2 Le renouvellement des autorisations

42. Le renouvellement des autorisations de mise en place d'un système de vidéoprotection pose certains problèmes d'ordre pratique.

43. En effet, l'autorisation doit être demandée auprès de la préfecture dont dépend la structure dans laquelle sera installé le système. Il faut donc faire une demande d'autorisation dans autant de préfecture qu'il peut y avoir potentiellement d'entités implantées dans différents départements.

44. Cette procédure peut donc s'avérer extrêmement lourde pour de grands groupes tels que la Société Générale qui compte 3000 sites différents.

45. Une fois la demande faite, une commission composée entre autre d'un magistrat, doit statuer sur le bien-fondé de la demande de mise en place du système. Cette commission doit se réunir tous les mois afin d'autoriser ou non le renouvellement des autorisations. Or, il peut arriver que certains magistrats aient des empêchements et ne puisse siéger. Des lors, il apparait que tenir une cette commission une fois par mois ne soit parfois pas possible, remettant l'autorisation de renouvellement des autorisations à plus tard.

46. De ce fait, la personne en charge des systèmes de vidéoprotection doit anticiper cette possibilité. De surcroit, c'est à lui de veiller au bon renouvèlement des autorisations dans le temps qu'il lui ai imparti (à savoir qu'une autorisation ne vaut que pour cinq ans). Aucun système d' « alarme » n'a en effet été mis en place afin de prévenir de la déchéance des autorisations.

2.3.3 Les normes techniques de l'arrêté du 3 août 2007 s'appliquant à la vidéoprotection

47. La demande d'autorisation se traduit par la présentation d'un dossier technique et administratif reposant sur les normes techniques de l'arrêté du 3 août 2007 qui, bien qu'obsolète est toujours en vigueur.

48. Depuis 2007, la vidéoprotection a bénéficié des innovations technologiques du numérique. Historiquement analogiques, les caméras ont évolué vers des enregistrements numériques, très largement privilégiés et qui se révèlent performants pour la qualité des saisies d'images et les supports de leur stockage.

49. Toutes ces évolutions n'ont pas été prises en compte par l'arrêté du 3 août 2007. De nouvelles caractéristiques techniques sont à définir pour assurer une qualité minimum des images et de leur transmission de sorte qu'elles puissent être exploitées dans de bonnes conditions par les forces de

[14] Cf. le site du Ministère de l'intérieur pour les informations pratiques, http://www.interieur.gouv.fr/

sécurité intérieure pour être en adéquation avec les nouvelles technologies. Sur cet aspect normatif, un travail a été réalisé par l'AN2V.

50. L'Association nationale de la vidéoprotection (AN2V) a réalisé en février 2014, un livre blanc pour une refonte des normes techniques de la vidéoprotection dans lequel elle propose des évolutions de ce texte permettant de satisfaire à la fois les exploitants, les fournisseurs, les pouvoirs publics et les services de sécurité intérieure[15].

2.3.4 Les dispositifs particuliers

51. Certaines autorisations peuvent être accordées en présence de situations d'urgence. La procédure d'autorisation en ce cas permet au préfet de délivrer une autorisation limitée dans le temps, de quatre mois maximum et ce, sans besoin de passer devant une commission, pour la mise en œuvre d'un système de vidéoprotection dans un lieu ouvert au public dans trois hypothèses :

- en cas d'urgence et ;
- en cas d'exposition particulière à des risques de terrorisme[16] ;
- en cas de manifestation ou de rassemblement de grande ampleur comportant des risques particuliers d'atteinte à la sécurité des personnes ou des biens[17].

52. Dans ce cas, il n'y a pas besoin de l'avis préalable de la commission départementale.

2.4 Systèmes de vidéoprotection relevant de la loi Informatique et Libertés

2.4.1 La déclaration à la Cnil

53. Les enregistrements de vidéoprotection sont considérés comme des données à caractère personnel, lesquelles sont soumises à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dès lors qu'elles sont utilisées pour la constitution de traitements dont la définition est donnée au point 2.2.

54. À ce titre, les traitements de vidéoprotection donnent lieu à une déclaration auprès de la Cnil[18]. Le défaut de déclaration fait l'objet de sanction (Code pénal, article 226-16).

55. Outre la déclaration, le responsable du traitement qui ne respecte pas les autres dispositions de la loi Informatique et libertés encoure des sanctions pénales en cas de :

- collecte déloyale ou illicite (Code pénal, article 226-18) ;
- durée de conservation excessive (Code pénal, article 226-20) ;
- détournement de la finalité du dispositif (Code pénal, article 226-21) ;
- absence d'information des personnes (Code pénal, article R625-10).

2.4.2 Les enregistrements sur un lieu de travail

56. En cas de vidéoprotection sur un lieu de travail, qu'il soit public ou privé, l'employeur doit informer les employés de l'utilisation d'un système de vidéoprotection et tout particulièrement, il doit respecter :

[15] Livre blanc AN2V – 13 Février 2014, http://www.an2v-pixel.com/
[16] CSI, art. L223-4 et art. L223-5.
[17] CSI, art. L252-7
[18] Cf. sur le site de la Cnil : http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/declaration-videosurveillance/

- la procédure d'information et de consultation des instances représentatives du personnel (entreprises de + de 50 salariés) (Code du travail, articles L2323-32 et L 4612-8 et s) ;
- la procédure d'information individuelle des salariés (Code du travail, articles L1221-9 et L1222-4) ;
- le principe de proportionnalité (Code du travail, article L1121-1).

57. Pour exemple, la Cnil, le 3 janvier 2013[19] a adopté une mise en demeure à l'encontre d'un syndicat de copropriétaire afin que soit supprimée la caméra servant à filmer le poste de sécurité des agents de sécurité du bâtiment.

58. La mise en demeure étant restée lettre morte, la formation restreinte de la Cnil a adopté à l'égard du syndicat, une sanction et une injonction de mettre un terme au caractère continu du traitement (la décision a par la suite été rendue publique), le système de vidéosurveillance ayant été jugé disproportionné.

59.Plus récemment, la Cour d'appel d'Aix-en-Provence a prononcé l'irrecevabilité en justice des enregistrements de vidéosurveillance à l'appui d'un licenciement pour vol sur le lieu de travail et condamné l'entreprise à verser 2 000 euros de dommages-intérêts au salarié[20]. La cour a rappelé les deux obligations de l'employeur en la matière :

- - informer les salariés de leur droit d'accéder aux enregistrements ;
- - détruire les enregistrements au terme de la durée de conservation déclarée à la Cnil.

2.4.3 Le respect de la vie privée

60. La législation relative au respect de la vie privée résulte de la loi du 17 juillet 1970 sur le droit à l'image (Code civil, article 9).

61. L'enregistrement de l'image d'une personne à son insu dans un lieu privé est pénalement sanctionné (Code pénal, article 226-1)[21].

2.4.4 Les dispositifs de reconnaissance faciale

62. Les enregistrements visuels de vidéoprotection qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[22].

63. C'est le cas des enregistrements visuels permettant la reconnaissance faciale notamment, du fait des fonctionnalités qu'ils comportent.

3. Systèmes relevant des deux régimes

64. Il est question ici de lieux particuliers où certains dispositifs peuvent dans un même espace avoir deux périmètres distincts.

65. Dans ce cas, le premier ministre rappelle la nécessité de faire application à la fois du code de la sécurité intérieure et de la loi du 6 janvier 1978, à savoir :

[19] Délibération 2012-475 du 03 janvier 2013 Syndicat des copropriétaires « Arcade des champs Elysées »
[20] CA Aix-en-Provence, 13 juin 2014, n°1/06776, SAS Logidis Comptoirs Modernes c/ D.
[21] Cf. sur le site de la Cnil : « Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », dossier du 21 juin 2012.
[22] CSI, art. L251-1.

- saisir le préfet territorialement compétent pour obtenir une autorisation préalable à l'installation d'un système et
- procéder auprès de la Commission nationale de l'informatique et des libertés à la formalité préalable applicable.

66. Un système de vidéoprotection dont certaines caméras filment l'intérieur d'un établissement non ouvert au public et d'autres visionnent ses abords immédiats ou une partie de l'établissement ouverte au public sera considéré comme un système mixte pouvant relever à la fois de la loi du 6 janvier 1978 pour les caméras filmant des personnes se trouvant habituellement dans l'établissement et aussi des dispositions des titres II (chapitre III) et V du livre II du code de la sécurité intérieure pour la ou les caméras filmant la voie publique.

67. Tel sera le cas d'un système dont certaines caméras filment les espaces d'un hôpital réservées aux seuls patients et d'autres filment le hall d'accueil et les abords extérieurs immédiats. Tel peut être aussi le cas en cas d'installation d'un système de vidéoprotection filmant une zone de caisse en magasin.

68. Ces systèmes de vidéoprotection mixtes sont soumis à autorisation préfectorale pour les parties ouvertes au public et à une saisine de la Cnil pour les parties non accessibles au public si, dans ces lieux, la majorité des personnes filmées sont reconnaissables par la personne chargée de visionner les images et si les images sont enregistrées.

3.1.1 La vidéoprotection aux abords des commerces

69. L'article 73 de la loi n°2014-626 du 18 juin 2014, loi « relative à l'artisanat, au commerce et aux très petites entreprises » vient compléter l'article L. 251-2 du code de la sécurité intérieure par un nouvel alinéa qui permet aux commerçants, après avoir informé le maire de la commune concernée et obtenu l'autorisation des autorités publiques compétentes, de mettre en œuvre sur la voie publique un système de vidéoprotection, pour protéger les abords immédiats de leurs installations.

70. Toutefois ce dispositif doit répondre à une finalité précise, celle « d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol ».

71. Il est par ailleurs à noter que des décrets prit en Conseil d'Etat viendront apporter des précisions quant aux modalités de mise en œuvre et aux types de bâtiments et installations qui seront concernés par cet article.

72. La nouvelle loi prévoit également de compléter l'article L. 252-2 du même code par un alinéa ainsi rédigé :

« Dans le cas prévu au dernier alinéa de l'article L. 251-2, le visionnage des images ne peut être assuré que par des agents de l'autorité publique individuellement désignés et habilités des services de police et de gendarmerie nationale ».

73. Ces dispositions limitent le visionnage des images aux agents de l'autorité publique. Les caméras seront aveugles pour les commerçants. En effet, le visionnage des images ne pourra être assuré que par des agents de l'autorité publique individuellement désignés, au risque d'une peine de 3 ans d'emprisonnement et 45 000 euros d'amende.

74. La notion « abord immédiat » pose beaucoup de question quant à sa définition. Il appartiendra à la jurisprudence d'en cerner les limites au cas par cas.

3.1.2 Les alertes commerçants

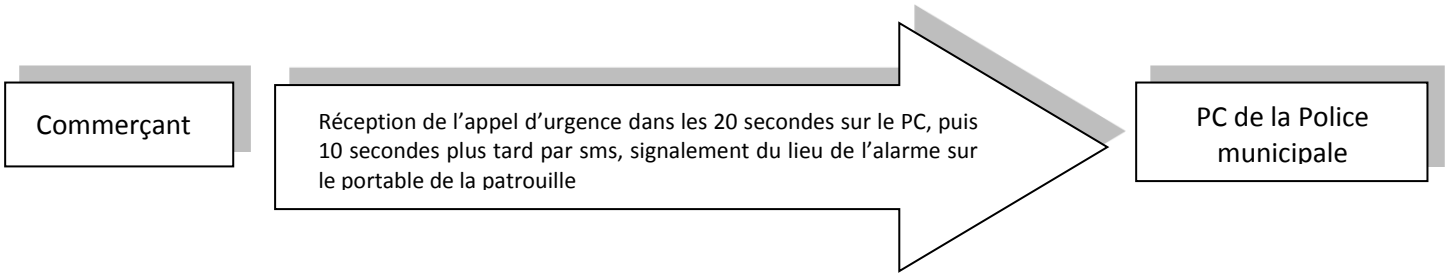
75. Sous l'impulsion de l'ancien ministre de l'intérieur M. Manuel Valls, de plus en plus de villes mettent en place que l'on appelle des « alertes commerçants ». Il s'agit de dispositifs reliant directement la police municipale à certains commerçants afin de permettre une intervention rapide des forces de l'ordre mais aussi, pour certains dispositifs, de permettre d'informer les commerçants se trouvant à proximité du lieu de l'agression ou du vol.

76. Il est dans un premier temps utile de rappeler que les commerces font partis des lieux privés, ouvert au public. C'est toutefois dans un but de sécurité publique qu'a été mis en place de genre d'alerte.

77. La mairie de Courcouronnes, ville située dans le département de l'Essonne a récemment mis en place un dispositif semblable.

78. Le dispositif s'appuie sur une convention[23] conclue entre la ville représentée par son maire et les commerçants. Le Maire s'engageant d'une part à assurer une permanence, s'assurer du bon fonctionnement du système et le commerçant à ne déclencher l'alerte qu'avec diligence, etc.

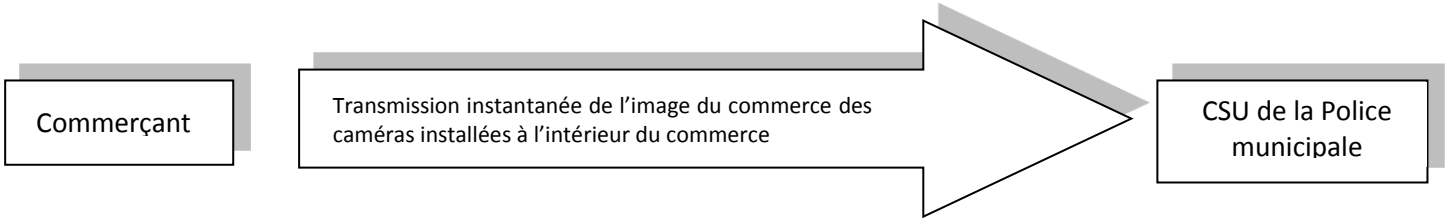
79. **Alerte par transmetteur téléphonique avec émetteur pendentif** :



- Appuie sur le bouton rouge du transmetteur disposé à proximité de la caisse
- Appuie sur le pendentif que le commerçant anormalement sur lui, portabilité d'à peu près 150 mètres

80.Toutefois ce dispositif ne permet de transmettre au poste de la Police municipale que les coordonnées du commerce et les sons.

81. **Alerte par vidéoprotection** :



82.Ce dispositif permet une transmission du son et de l'image.

83.Il peut donc choisir soit, en cas de braquage ou d'agression immédiate d'avertir les forces de l'ordre pour une intervention ou, si il ne constate pas de problèmes, de prendre contact avec le commerçant afin de connaître les motifs pour lesquels ce dernier a utilisé le dispositif.

[23] Voir Annexe du présent livre blanc.

84. Dans les deux cas il n'y a donc pas d'enregistrement et/ou de transmission continue. Il s'agit bien d'un dispositif que le commerçant doit déclencher.

85. Concernant la prise en charge financière, ce type de système est intéressant pour le commerçant. S'agissant de l'installation permettant une vidéoprotection, l'acquisition et la maintenance du matériel sont à la charge du commerçant. S'agissant du transmetteur téléphonique, la ville prend en charge l'acquisition du logiciel et de sa maintenance.

86. Les interventions de la police municipale, faisant suite au déclenchement de l'alerte, entrainent une intervention prioritaire effectuée dans le cadre de la sécurité publique et de la protection des commerces de proximité et non pour un autre évènement intervenant sur la voie publique.

3.1.3 Le cas particulier des buralistes

87. Le décret n° 2012-1448 du 24 décembre 2012 relatif à l'aide à la sécurité des débits de tabac est venu modifier le décret du 27 juin 2006 et a pour objet l'octroi de subventions par l'Etat au bénéfice des débitants de tabac, visant à renforcer la protection des débits contre les vols.

88. Dans cette optique, chaque débit de tabac, après avoir passé un audit de sécurité afin de déterminer le coût de l'installation de protection envisagée, pourra en adressant une demande auprès de la Direction interrégionale des douanes compétente recevoir une subvention.

89. Le directeur interrégional des douanes détermine le montant de l'aide en fonction du devis sur lequel figure l'offre économiquement la plus avantageuse au regard du prix, même si le demandeur retient un autre devis. La subvention est égale à 80 % du coût HT et 50 % de l'audit de sécurité peut être imputé de cette première. Toutefois la subvention en tout état de cause ne pourra pas dépasser 15 000 €.

3.1.4 La délimitation des périmètres et le partage des responsabilités

90. Tous les acteurs ont un rôle à jouer et/ou une certaine responsabilité. Ainsi, l'installateur a un devoir de conseil auprès du donneur d'ordre qui est lui-même responsable du traitement lors de la mise en place de dispositifs.

91. Il en ressort que, dans certains cas, notamment dans le cadre des Etablissements recevant du public (ERP), des interrogations subsistent encore quant au choix entre l'autorisation préfectorale ou la déclaration Cnil ; or celles-ci entraînent des obligations très différentes.

3.1.5 Le régime juridique du contrôle a posteriori

92. A l'occasion d'une question parlementaire écrite N° 85925[24], le ministère de la Justice et des libertés a rappelé le double régime juridique du contrôle a posteriori des systèmes de vidéoprotection depuis la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2), modifiant l'article 10 de la loi du 10 janvier 1995 :

- Lorsque l'installation du dispositif a été autorisée par le représentant de l'État dans le département, ou le préfet de police à Paris, le pouvoir de contrôle de ces installations relève de la commission départementale de vidéoprotection compétente. Celle-ci peut, à tout moment, contrôler les conditions de fonctionnement du dispositif, à savoir notamment les éléments relatifs à l'enregistrement et à la durée de conservation des images. Elle émet, le cas échéant, des recommandations et propose la suspension ou la suppression des dispositifs

[24] Réponse publiée au JO Ass. nat. du 23-8-2011 : http://questions.assemblee-nationale.fr/q13/13-85925QE.htm
Cf annexe 4 du présent livre blanc.

non autorisés, non conformes à leur autorisation ou dont il est fait un usage anormal. Elle informe le maire de la commune concernée.

- En revanche, si la mise en œuvre d'un tel système a été autorisée par la Commission nationale de l'informatique et des libertés, celle-ci dispose de l'intégralité de son pouvoir d'enquête et de sanction, afin de s'assurer du respect de la déclaration ou de l'autorisation effectuée pour les enregistrements.

- Par ailleurs, la Cnil peut, sur demande de la commission départementale compétente, du responsable d'un système ou de sa propre initiative, exercer un contrôle visant à s'assurer que le système est utilisé conformément à son autorisation et, selon le régime juridique dont le système relève, aux dispositions de la loi du 10 janvier 1995 susvisée ou à celles de la loi du 6 janvier 1978 modifiée.

- Lorsque la Cnil constate un manquement aux dispositions de la loi du 10 janvier 1995 susvisée, elle peut, après avoir mis en demeure la personne responsable du système de se mettre en conformité, dans un délai qu'elle fixe, demander au représentant de l'État dans le département et, à Paris, au préfet de police, d'ordonner la suspension ou la suppression du système de vidéoprotection. Elle informe le maire de la commune concernée de cette demande (Loi n°2011-267 du 14-3-2011, art. 18).

4. Sous-groupe : Droit d'accès et conservation des images

4.1 Principes et règles applicables

93. L'article L.253-5 du Code de la sécurité intérieure consacre un droit d'accès aux images au profit de toute personne susceptible d'avoir été filmée par un système de vidéoprotection.

94. Toute personne intéressée peut ainsi s'adresser au responsable d'un système de vidéoprotection afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit[25].

95. La conservation des images ne peut pas dépasser 1 mois, sauf procédure judiciaire en cours.

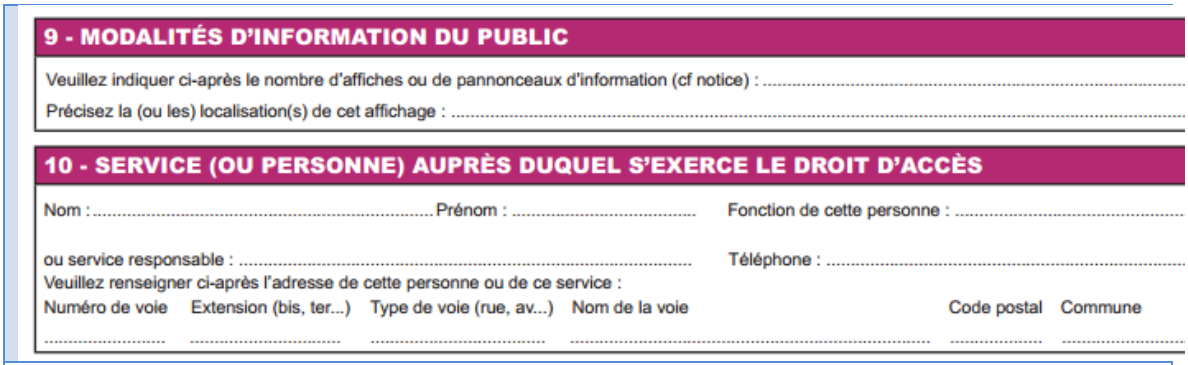
96. La demande d'accès doit être adressée au responsable du système de vidéoprotection désigné et habilité à traiter cette procédure.

4.1.1 L'information relative au droit d'accès aux enregistrements vidéo

97. Les personnes filmées doivent être informées, au moyen de panneaux affichés de façon visible :
- de l'existence du dispositif,
- de son responsable,
- des modalités concrètes d'exercice de leur droit
- d'accès aux enregistrements visuels les concernant.

98. Ces informations sont à fournir au préfet lors de la demande d'autorisation d'installation (formulaires cerfa n°13806-03 et cerfa n°14095-02 pour un établissement bancaire)[26] :

[25] Code de la sécurité intérieure, art. L253-5.
[26] Cf. le site du Ministère de l'intérieur pour les informations pratiques, http://www.interieur.gouv.fr/



9 - MODALITÉS D'INFORMATION DU PUBLIC

Veuillez indiquer ci-après le nombre d'affiches ou de pannonceaux d'information (cf notice) : .....

Précisez la (ou les) localisation(s) de cet affichage : .....

10 - SERVICE (OU PERSONNE) AUPRÈS DUQUEL S'EXERCE LE DROIT D'ACCÈS

Nom : ..... Prénom : ..... Fonction de cette personne : .....

ou service responsable : ..... Téléphone : .....

Veuillez renseigner ci-après l'adresse de cette personne ou de ce service :

Numéro de voie | Extension (bis, ter...) | Type de voie (rue, av...) | Nom de la voie | Code postal | Commune

Extrait des formulaires cerfa n°13806-03 et cerfa n°14095-02

99. Ces informations doivent également figurer dans les panneaux qui sont affichés en permanence dans les lieux concernés et doivent être compréhensibles par tous les publics.

100.Cette mention peut toutefois ne pas être suffisante à l'égard des salariés de l'établissement dans lequel un système de vidéoprotection est installé.

101. Ainsi, dans un arrêt en date du 13 juin 2014, la Cour d'appel d'Aix-en-Provence a considéré que l'affichage dans les locaux de l'entreprise de la mention « surveillance vidéo 24/24h décret 96-926 du 17 octobre 1996 » était insuffisante en ce qu'elle n'informait pas le salarié de son droit d'accès prévu par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

102. En l'espèce, un salarié licencié pour un vol sur son lieu de travail contestait la licéité des enregistrements vidéo versés au débat par l'employeur et demandait réparation du préjudice causé par cette faute contractuelle.

103. La Cour d'appel d'Aix-en-Provence a prononcé l'irrecevabilité en justice des enregistrements de vidéosurveillance et condamné l'entreprise à verser 2 000 euros de dommages-intérêts au salarié[27].

4.1.2 L'exercice du droit d'accès aux enregistrements vidéo

104. Le demandeur n'est pas tenu d'invoquer un préjudice quelconque ni de motiver sa demande.

105. En pratique, ce droit d'accès permet aux citoyens de s'assurer que les images les concernant n'ont pas été conservées au-delà du délai fixé dans l'arrêté d'autorisation.

106. La réglementation impose au responsable du traitement de tenir un registre comme élément de preuve de la destruction des enregistrements dans le délai requis.

107. Ce registre, qui contient la mention des enregistrements réalisés, la date de destruction des images et, le cas échéant, celle de leur transmission au parquet, doit pouvoir être présenté à toute réquisition de l'autorité chargée du contrôle de la conformité du système.

108. La circulaire du 12 mars 2009 relative aux conditions de déploiement des systèmes de vidéoprotection préconise aux préfets d'encourager le responsable à y faire également figurer la mention des transmissions réalisées au profit de services agissant dans le cadre de missions de police administrative.

4.1.3 Le refus d'accès

109. Bien que l'accès aux enregistrements soit un droit, un refus d'accès peut toutefois être opposé :

[27] CA Aix-en-Provence, 13 juin 2014, n°1/06776, SAS Logidis Comptoirs Modernes c/ D.

- dans le cas où le demandeur demande à accéder à des enregistrements qui ne le concernent pas ;
- pour des motifs limitativement énoncés par la loi ;
- en cas d'instruction judiciaire.

110. Ne peuvent donc être rejetées que les demandes qui porteraient atteinte à la sûreté de l'Etat, compromettraient la défense ou la sécurité publique, nuiraient au déroulement de procédures engagées devant les juridictions ou aux opérations préliminaires à de telles procédures ou affecteraient le droit des tiers filmés au respect de leur vie privée[28].

4.1.4 Le contrôle et les recours en cas de difficulté d'accès

111. Les instances de recours :

1. La Commission départementale des systèmes de vidéoprotection
2. La Commission nationale de l'informatique et des libertés (Cnil)
3. Le recours devant le juge

4.1.5 La Commission départementale des systèmes de vidéoprotection

112. Toute personne rencontrant une difficulté dans le fonctionnement d'un système de vidéoprotection peut saisir la commission départementale des systèmes de vidéoprotection[29].

113. Cette instance peut aussi, en dehors de toute saisine de particuliers, décider d'exercer un contrôle des systèmes (sauf en matière de défense nationale).

114. Elle peut également émettre des recommandations, proposer la suspension ou la suppression des dispositifs non autorisés. Elle informe le maire de la commune de cette proposition.

115. La circulaire du 12 mars 2009 relative aux conditions de déploiement des systèmes de vidéoprotection prévoit que « la saisine de la commission par un citoyen peut porter non seulement sur un problème d'accès aux images mais sur toute question liée au fonctionnement du système, par exemple, sur le contrôle de la destruction des images ».

4.1.6 La Commission nationale de l'informatique et des libertés (Cnil)

116. La Cnil peut, sur demande de la commission départementale des systèmes de vidéoprotection, du responsable du système ou de sa propre initiative, exercer un contrôle visant à s'assurer que le système est utilisé conformément à son autorisation et aux dispositions de la loi.

117. Si elle constate un manquement, elle peut, après mise en demeure du responsable du système de se mettre en conformité, demander au préfet d'ordonner la suspension ou la suppression du système. Elle informe le maire de la commune concernée de cette demande.

4.1.7 Le recours devant le juge

118. La saisine de la Commission départementale des systèmes de vidéoprotection ou de la Commission nationale de l'informatique et des libertés ne constitue pas le préalable obligatoire à l'exercice d'un recours administratif ou contentieux.

[28] Code de la sécurité intérieure, art. L253-5.
[29] Code de la sécurité intérieure, art. L253-5.

119. Que l'une ou l'autre des commissions aient été saisies ou non, toute personne peut s'adresser à la juridiction compétente, au besoin en la forme du référé[30], en cas de difficultés concernant un système de vidéoprotection.

120. Il peut s'agir du juge administratif ou du juge judiciaire, suivant les situations et l'objet du recours (notamment qualité publique ou privée de la personne responsable du système, recours en annulation de l'autorisation préfectorale, poursuites pénales, etc.).

121. L'intéressé peut déposer, s'il le juge nécessaire, une demande en référé.

4.2 Les difficultés de mise en œuvre

122. En matière enregistrements vidéo, le droit d'accès est assez difficile à mettre en œuvre car une demande d'accès ne peut être traitée que par un personnel habilité, l'accès aux images et enregistrements étant réservé aux seuls agents des services de police et agents municipaux individuellement désignés.

4.2.1 Absence de formalisme

123. Tel que prévu par le Code de la sécurité intérieure, ce droit n'est pas aisé à mettre en œuvre car la procédure d'une demande d'accès n'est pas réellement formalisée sur le plan pratique. Ce qui suscite de nombreuses questions :

- Doit-elle être faite sur place uniquement ? oralement ou à l'aide d'un formulaire ?
- Peut-elle être faite par courrier postal ou électronique ?
- Comment est faite l'authentification du demandeur ? Quels justificatifs d'identité faut-il fournir ?
- Peut-elle être faite par une société ? un tiers mandaté ? si oui, sous quelle forme ?
- La réception d'une demande écrite proroge-t-elle le délai de conservation des images ?
- Quel est le délai de réponse ?
- Quelles sont les limites ? (demandes abusives)
- Est-elle consignée dans un registre ?
- La décision de refus doit-elle être dûment motivée ?
- etc.

124. Ce droit est très difficile à mettre en pratique. En effet, il n'est formalisé par aucun texte, ce qui laisse toute liberté aux responsables de systèmes de vidéoprotection sur la procédure à mettre en place pour exercer ce droit (demande formulée par voie orale ou écrite, personnelle ou mandatée par un tiers, délai de réponse, etc.).

125. Mais il reste encore à définir des points importants pour l'exercice du droit d'accès :

- Combien de minutes de vidéos un demandeur peut-il visionner ?
- Combien de caméra un demandeur peut-il demander ?
- Combien de demande de droit d'accès un demandeur peut-il déposer auprès du même responsable de système de vidéoprotection (proportionnalité de la demande) ?

126. La procédure à mettre en place est laissée à l'appréciation et aux moyens dont disposent les organismes ayant à traiter les demandes. Ces dernières sont donc différemment traitées d'un organisme à l'autre.

[30] Code de la sécurité intérieure, art. L253-5.

4.2.2 Difficultés techniques

127. Une difficulté technique complexe et coûteuse : pour flouter certaines zones (protection de la vie privée), pour disposer de moyens financiers, humains etc. alloués au traitement des demandes de droit d'accès.

128. Comme rappelé précédemment, le droit d'accès est de droit. Cependant, lorsqu'une personne souhaite exercer son droit d'accès, il est nécessaire de s'assurer de certains points, d'une part pour disposer de renseignements afin de traiter la demande et d'autre part, pour s'assurer que la personne est bien concernée par les images qu'elle demande, qu'il n'y a pas d'atteinte à la vie privée de tiers.

129. Lorsqu'une personne souhaite accéder à des images de vidéoprotection, il faut :

- vérifier que les enregistrements demandés la concernent bien en s'assurant de son identité (déclaration sur l'honneur ou visuelle à partir d'un titre d'identité, de photo récente, etc.), de la date, de l'heure et du contexte dans lesquels ont été réalisés les enregistrements ;
- travailler les enregistrements, c'est-à-dire isoler la personne concernée en floutant toutes les autres personnes figurant sur les enregistrements (protection de la vie privée) ;
- assurer la traçabilité de l'accès et de la destruction des enregistrements demandés par la personne.

130. Ces opérations qui peuvent prendre un certain temps ne peuvent être réalisées que par un représentant de police, expressément habilité à accéder aux images.

131. Même si des logiciels existent pour extraire les images d'une séquence, c'est uniquement après un important et coûteux travail préalable de recherche qui n'est pas à la portée de toute institution.

4.3 Exemples de traitements du droit d'accès

4.3.1 La procédure mise en place par la Préfecture de police de Paris (MIVAP)

132. Les demandes d'accès émanant de particuliers sont croissantes depuis la mise en place du plan de vidéoprotection pour Paris (PVPP). La MIVAP est la cellule au sein de la Direction Opérationnelle des Services Techniques et Logistiques de la Préfecture de Police de Paris en charge du traitement des demandes de droit d'accès pour les images issues du PVPP.

133.Un peu plus d'une centaine de demandes de droit d'accès par an est traitée par la MIVAP. Elles sont traitées au cas par cas et posent parfois des difficultés quant à l'étendu du droit d'accès prévu par la loi.

134. La Mission pour le développement de la Vidéoprotection en Agglomération Parisienne a mis en place une procédure de traitement des demandes d'accès.

135. Le délai de conservation des images est de 30 jours, sauf en cas d'enquête judiciaire.

136. Le tiers demandeur peut effectuer une demande via le formulaire disponible sur le site internet « monservicepubli.fr » (ci-dessous point 4.3.2).

137. Il peut également laisser un message sur la ligne téléphonique dédiée : 01 40 79 71 71.

138. Il peut enfin adresser sa demande par courrier, à l'attention du Préfet de Police. Les demandes faites par écrit sont rares.

139. Quel que soit le support de la demande, la MIVAP prend contact avec le demandeur pour obtenir des renseignements complémentaires sur sa demande, notamment, le contexte afin de reconnaître le demandeur sur les images ou des éléments (une voiture, un lieu, une situation etc.) permettant d'établir si le demandeur est bien concerné par la demande et de vérifier, protéger le droit des tiers.

140. Bien évidemment, certaines demandes nécessitent un travail de recherche plus important : un demandeur peut ne donner qu'une adresse ou un lieu, alors il faudra rechercher les caméras susceptibles d'avoir filmées la scène ; un demandeur peut fournir une plage horaire importante (par exemple la dégradation de sa voiture entre 00h et 8h).

141. Dans tous les cas la MIVAP prend le temps d'affiner la recherche pour répondre au plus près à la demande.

142.La demande est réceptionnée directement et traitée par le service compétent (Mission pour le développement de la Vidéoprotection en Agglomération Parisienne - MIVAP).

143. La MIVAP prend contact avec le tiers demandeur pour obtenir des renseignements complémentaires sur sa demande, notamment, le contexte de la demande afin de reconnaître le tiers demandeur sur les images où les autres éléments de contexte (une voiture, un lieu, une situation, etc.).

144. Tout au long de l'examen de sa demande, le tiers demandeur est informé de l'avancée et des différents états de sa demande : dossier reçu, transmis au service traitant, en cours de traitement, accepté, refusé et clos). Il est, principalement, contacté par courrier électronique, notamment pour l'informer de l'acceptation ou du refus de sa demande.

145. Dans le cas d'une réponse positive, le tiers demandeur est invité à consulter ses enregistrements avant l'expiration du délai de conservation des 30 jours.

146. Dans tous les cas, aucune séquence extraite du système de captage vidéo, sous quelque forme que ce soit, ne lui est remise.

147. La Mivap conserve ses éléments à des fins statistiques. Le comité d'éthique est informé, mensuellement, de toutes les demandes de droit d'accès. Ces données ne sont, actuellement, pas disponibles, ni publiées.

148. Un registre de suivi des demandes de droit personnel d'accès aux enregistrements a été mis en place.

149. De nombreux cas sont recensés, pour lesquels ce droit d'accès a été refusé :

- Absence d'images : caméra non opérationnelle à la date de la demande ou demande effectuée dans un délai supérieur de 30 jours après l'enregistrement effectué.

- Enquête judiciaire en cours.

- Demande formulée par un tiers et non la personne concernée.

150. Bien que rien ne soit expressément prévu dans la loi en ce qui concerne les demandes d'accès exercées par un tiers mandaté, deux cas de refus ont été rapportés par la MIVAP :

- Une demande a été formulée par un avocat pour son client. La MIVAP a considéré que cette demande ne pouvait être recevable, la personne concernée devant seule réclamer l'accès.

- Un tiers demandeur a effectué une demande pour sa mère, dans l'incapacité temporaire de se déplacer à la suite d'un accident. La MIVAP a refusé la demande pour enquête judiciaire en cours.

151. Depuis la mise en place du PVPP, un peu plus d'une centaine de demande de droit d'accès par an est traitée par la MIVAP.

152. On note que la vidéoprotection rentre dans les mœurs et devient un réflexe autant pour les forces de polices que pour les administrés, que l'une des premières raisons du secours à la vidéoprotection pour les administrés est l'exploitation des images.

153. Une plaquette d'information sur le PVPP est disponible dans tous les commissariats.

4.3.2 Formulaire en ligne de droit personnel d'accès aux enregistrements de vidéoprotection de la Préfecture de police de Paris (MIVAP)

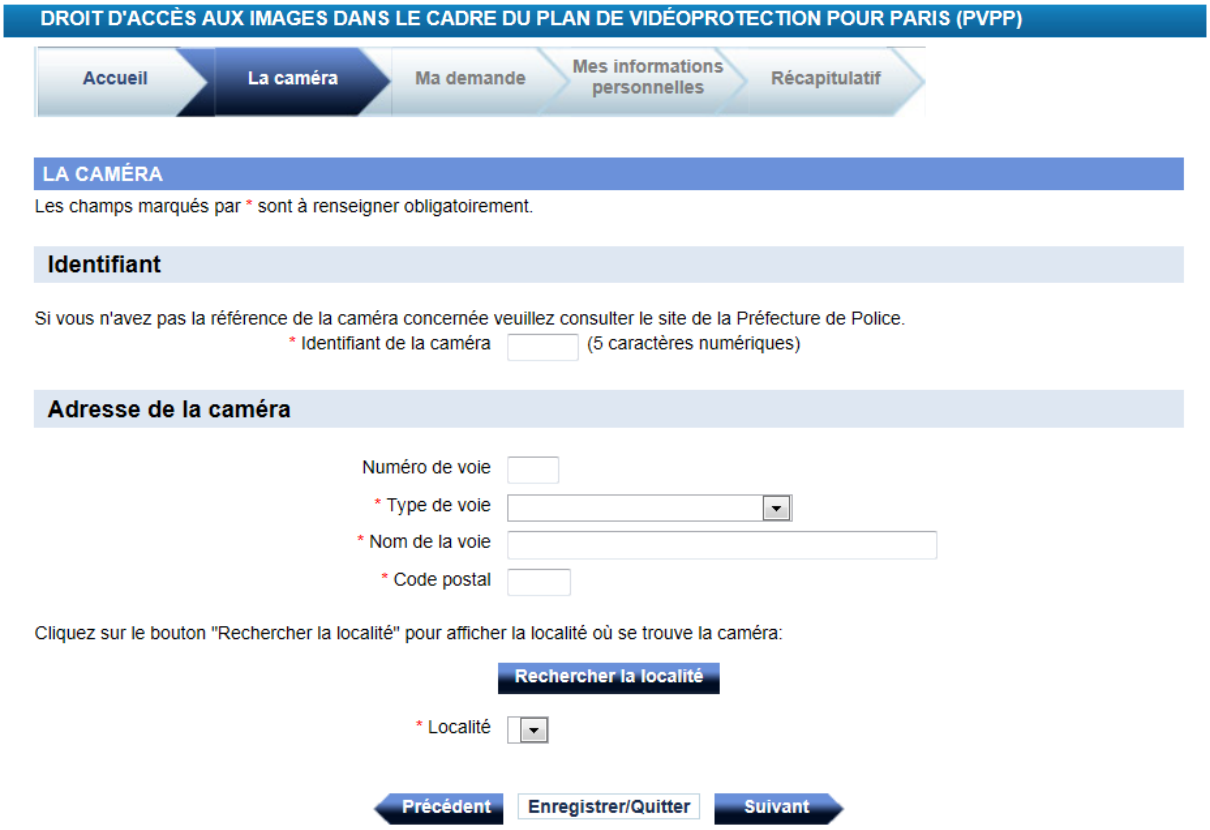
154. Le formulaire de droit d'accès est disponible sur le site internet « monservicepubli.fr » en cliquant sur les liens suivants :

https://mon.service-public.fr/portail/app/cms/public/les_demarches?page=2

et en s'inscrivant sur le site : https://mdel.mon.service-public.fr/plan-de-videoprotection-pour-paris-pvpp.html

155. Cette démarche demande environ 15 minutes pour être réalisée en suivant les étapes suivantes :

- La caméra
- La demande
- Les informations personnelles du demandeur



DROIT D'ACCÈS AUX IMAGES DANS LE CADRE DU PLAN DE VIDÉOPROTECTION POUR PARIS (PVPP)

Accueil | La caméra | Ma demande | Mes informations personnelles | Récapitulatif

LA CAMÉRA

Les champs marqués par * sont à renseigner obligatoirement.

Identifiant

Si vous n'avez pas la référence de la caméra concernée veuillez consulter le site de la Préfecture de Police.

* Identifiant de la caméra (5 caractères numériques)

Adresse de la caméra

Numéro de voie

* Type de voie

* Nom de la voie

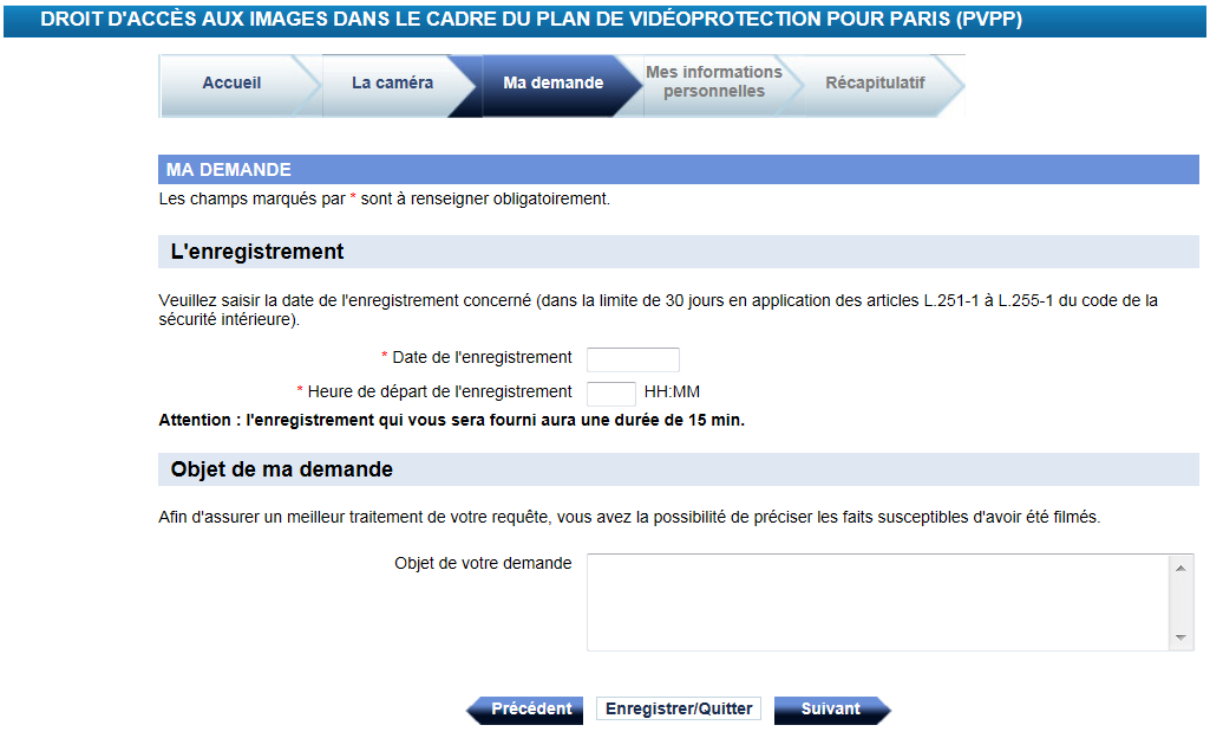
* Code postal

Cliquez sur le bouton "Rechercher la localité" pour afficher la localité où se trouve la caméra:

Rechercher la localité

* Localité

Précédent | Enregistrer/Quitter | Suivant



DROIT D'ACCÈS AUX IMAGES DANS LE CADRE DU PLAN DE VIDÉOPROTECTION POUR PARIS (PVPP)

Accueil | La caméra | Ma demande | Mes informations personnelles | Récapitulatif

MA DEMANDE

Les champs marqués par * sont à renseigner obligatoirement.

L'enregistrement

Veuillez saisir la date de l'enregistrement concerné (dans la limite de 30 jours en application des articles L.251-1 à L.255-1 du code de la sécurité intérieure).

* Date de l'enregistrement

* Heure de départ de l'enregistrement HH:MM

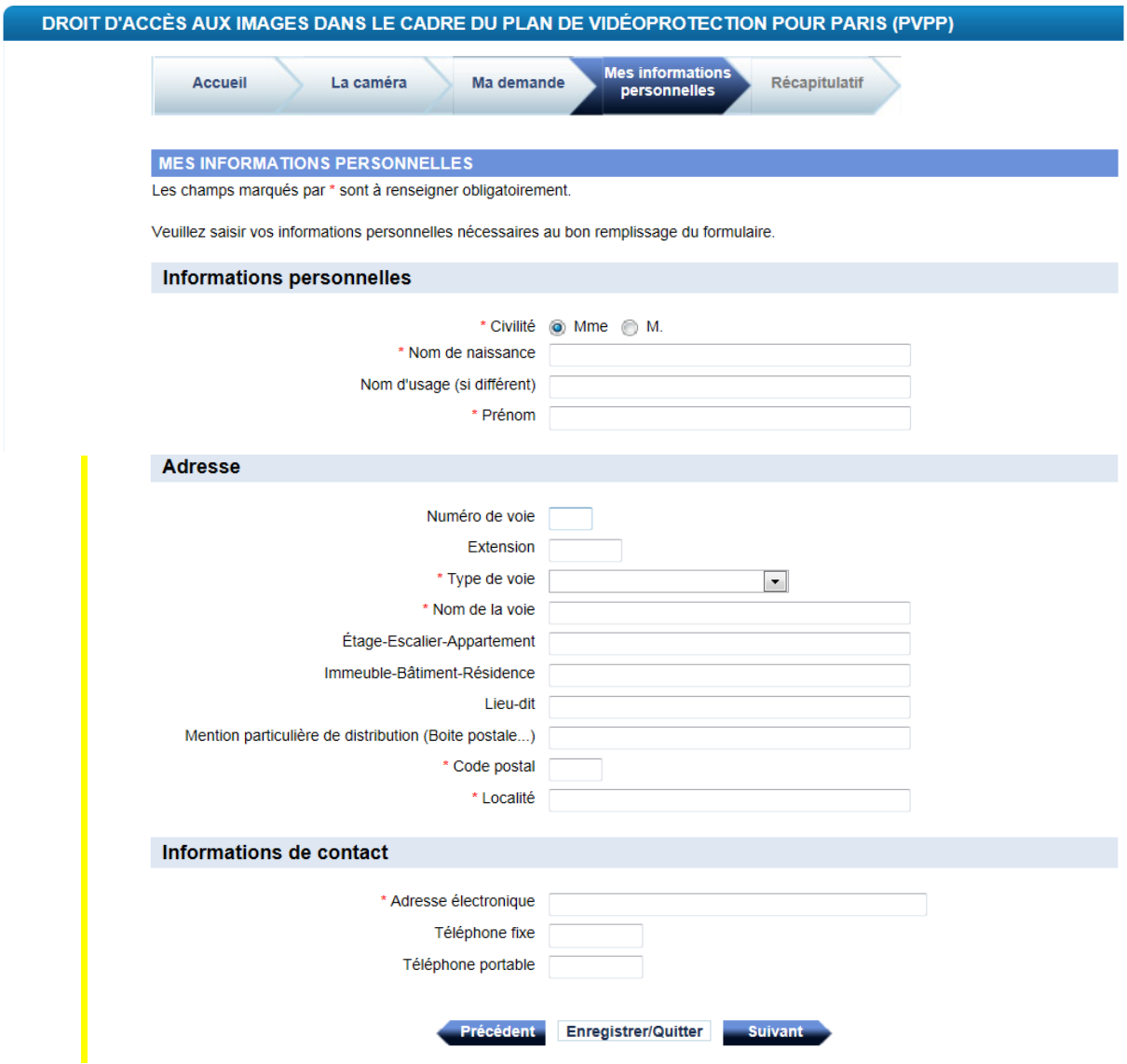
Attention : l'enregistrement qui vous sera fourni aura une durée de 15 min.

Objet de ma demande

Afin d'assurer un meilleur traitement de votre requête, vous avez la possibilité de préciser les faits susceptibles d'avoir été filmés.

Objet de votre demande

Précédent | Enregistrer/Quitter | Suivant


DROIT D'ACCÈS AUX IMAGES DANS LE CADRE DU PLAN DE VIDÉOPROTECTION POUR PARIS (PVPP)
Accueil
La caméra
Ma demande
Mes informations personnelles
Récapitulatif
MES INFORMATIONS PERSONNELLES
Les champs marqués par * sont à renseigner obligatoirement.
Veuillez saisir vos informations personnelles nécessaires au bon remplissage du formulaire.
Informations personnelles
* Civilité Mme M.
* Nom de naissance
Nom d'usage (si différent)
* Prénom
Adresse
Numéro de voie
Extension
* Type de voie
* Nom de la voie
Étage-Escalier-Appartement
Immeuble-Bâtiment-Résidence
Lieu-dit
Mention particulière de distribution (Boite postale...)
* Code postal
* Localité
Informations de contact
* Adresse électronique
Téléphone fixe
Téléphone portable
Précédent
Enregistrer/Quitter
Suivant

4.3.3 Cas d'illustrations du traitement des demandes de droit d'accès aux images issues du PVPP

Le demandeur :	Thème de la demande :	Motif de la demande :	Objectif de la demande :	Demande de droit d'accès :	Le demandeur a visionné les images :	Remarque :
M.S	Accident	Accident de moto. Refus de l'automobiliste de faire un constat	Déterminer les responsabilités en matière d'assurance	Favorable	n'a pas donné suite	
Mme BA	Accident	Accident de voitures	Déterminer les responsabilités en matière d'assurance	Favorable	Oui	
M.C	Accident	Accident de voitures	Déterminer les responsabilités en matière d'assurance	Refusé : délai de conservation dépassé	_	
Mme C	Accident	Piétonne renversée par une voiture	Déterminer les responsabilités en matière d'assurance	Favorable	Oui	
M. et Mme B	Accident	Accident de voitures	Déterminer les responsabilités en matière d'assurance	Favorable	n'a pas donné suite	
M.R	Accident	Accident de voitures	Déterminer les responsabilités en matière d'assurance	Favorable	Oui	
M.F	Violence aux personnes	Un individu a suivi sa fille à la sortie du collège	Reconnaître les individus	Refusé : pas de caméras PVPP à proximité	_	
M.B	Violence aux personnes	Altercation entre personnes et intervention de police	Comprendre les circonstances de l'altercation	Refusé : procédure judiciaire en cours	–	

M.G	Contestation de verbalisation	L'automobiliste s'est fait verbalisé pour franchissement de feu rouge	Contester la verbalisation	Refusé : délai de conservation dépassé	–	
M. et Mme D	Vol	Vol de chien avec dépôt de plainte	Reconnaître les individus	Refusé : procédure judiciaire en cours	–	
M. RM	Vol	Vol d'enseigne lumineuse de taxi sans dépôt de plainte	Reconnaître les individus	Favorable	n'a pas donné suite	
Depuis mars 2014						
M. TG	Vol	Vol de moto	Reconnaître les individus	Favorable	Oui	Pas d'élément exploitable pour le demandeur : la caméra n'a pas filmé le moment du vol
Mme MS	Vol	Vol d'une tablette numérique lors d'un rendez-vous fixé pour la vente de celle-ci	Reconnaître les individus	Refusé : pas de caméras PVPP à proximité	–	Le voleur est parti en direction du Palais des Congrès. Mme SC a exercé son droit d'accès auprès du Palais des Congrès qui a refusé, aux motifs qu'il ne pouvait donner accès aux images que par réquisition des forces de police.
Mme EV	Accident	Piétonne renversée par une voiture	Prendre la plaque d'immatriculation du véhicule qui l'a renversée	Favorable	Oui	Pas d'élément exploitable pour le demandeur : plaque d'immatriculation illisible

Mme BA	Accident	Société d'assurance exerçant le droit d'accès de l'un de ses clients	Connaître les circonstances de l'accident	Refusé	–	
M. D	Vol	Vol d'ordinateur portable dans camion de livraison	Reconnaître les individus	Favorable	n'a pas donné suite	
M. DP	Accident	Conducteur de scooter renversé par une voiture	Comprendre les circonstances de l'accident	Favorable	Oui	Les images ont permis au demandeur de mieux comprendre l'accident
Mme NH	Problèmes avec son employeur	La demandeuse est accusée par son employeur d'abandon de poste.	La demandeuse souhaite voir les images pour prouver qu'elle était, à ce moment, en livraison pour son employeur	La demandeuse a renoncé à exercer son droit d'accès	–	Le conflit de la demandeuse avec son employeur s'est résolu, ce dernier a accepté de lui payer ses heures de travail
M. JJ	Accident	Accident de voitures	Comprendre les circonstances de l'accident	Favorable	Oui	Les images ont permis au demandeur de mieux comprendre l'accident
Mme AS	Verbalisation	La demandeuse a été verbalisée par des agents de la RATP dans le métro	Contester la verbalisation	Refusé : pas de caméras PVPP à proximité	–	La demandeuse a été orientée vers la RATP
M. CM	Verbalisation	Vol de téléphone portable dans camion de livraison	Reconnaître les individus	Favorable	n'a pas donné suite	L'extraction des images a été demandée par les forces de police, suite au dépôt de plainte du demandeur

4.3.4 La procédure mise en place par la SNCF

156. La SNCF qui procède à l'aide d'un formulaire écrit de demande d'accès (contenu). La demande peut être faite sur papier libre ou sur le formulaire établi par SNCF.

157. Le tiers demandeur restitue (par voie postale ou à un guichet) le formulaire complété (ou sa demande sur papier libre) et accompagné d'une photo d'identité récente afin de faciliter les recherches.

158. A réception, la demande est transmise aux agents habilités vidéo de la Surveillance Générale SNCF qui procèdent aux recherches utiles.

159. Les contacts avec le tiers demandeur relèvent de l'exploitant du système ou d'un représentant Sûreté (autre que la Surveillance Générale).

160. A l'issue des recherches et que soit la nature de la réponse, le tiers demandeur est contacté par téléphone, puis il reçoit une confirmation écrite à l'aide du talon réponse du formulaire.

161. Dans le cas d'une réponse positive, le tiers demandeur est invité à consulté ses enregistrements, dans la limite du délai de 30 jours date des faits. Après visionnage des enregistrements, ceux-ci sont détruits en présence du demandeur.

162. Dans tous les cas, la photo d'identité est restituée au demandeur et aucune séquence extraite du système de captage vidéo, sous quelle que forme que ce soit, ne lui est remise.

163. Un registre de suivi des demandes de droit personnel d'accès aux enregistrements est mis en place en local ou en région. Le modèle générique de ce registre a fait l'objet d'une déclaration au CIL de l'entreprise.

164. A ce jour, les demandes d'accès émanant de particuliers restent marginales.

165. Deux cas sont recensés, au niveau de la SNCF, pour lesquels ce droit d'accès a été refusé :

- -Une demande a été effectuée dans un délai supérieur à 72 heures après l'enregistrement effectué.
- -Enquête judiciaire en cours.

4.3.5 Formulaires SNCF de droit personnel d'accès aux enregistrements de vidéoprotection

166. Le formulaire de demande :

DEMANDE DE DROIT PERSONNEL D'ACCES AUX ENREGISTREMENTS DE VIDEOPROTECTION.

(Article L.253-5 du Code de la Sécurité Intérieure)

IDENTITE DU DEMANDEUR :
NOM : ..... PRENOM : .....
ADRESSE : .....
Téléphone : ..... Date de naissance (1) : .....

Important : Le demandeur doit impérativement fournir une photo d'identité récente (2)

CIRCONSTANCES EVENTUELLEMENT ENREGISTREES :
GARE / TRAIN VIDEOPROTEGE : .....
DATE : .....
HEURE : de.....à .....
LIEU PRECIS Gare de (Quai n°- Hall – Souterrain): .....
LIEU PRECIS : Train N° voiture N° Train en direction de .....
Gare et heure de départ du demandeur :.....

Date et signature du demandeur :

167. Le formulaire de réponse :

TALON REPONSE A UNE DEMANDE DE DROIT PERSONNEL D'ACCES AUX ENREGISTREMENTS DE VIDEOPROTECTION.

Madame, Monsieur .....
Suite à votre demande personnelle de visionnage d'images de vidéoprotection formulée dans le cadre de l'article L.253-5 du Code de la Sécurité Intérieure, je vous prie de bien vouloir prendre connaissance des informations suivantes :

☐ Evènement non enregistré
☐ Enregistrement détruit le .....
☐ Demandeur non visualisé sur les enregistrements
☐ Enregistrement non communicable :
- o enregistrement intéressant la sûreté de l'Etat, la Défense ou la Sécurité Publique
- o procédure judiciaire en cours
- o protection de la vie privée d'un tiers

☐ Demandeur visualisé sur les enregistrements : L'intéressé est invité à visualiser les images correspondantes le (date et heure)..... au lieu ci-après .....
.....
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes meilleures salutations.

Le Responsable Local Vidéoprotection

(1) Le demandeur mineur doit être assisté dans sa demande par son représentant légal.
(2) Permettre l'identification lors des recherches

4.4 Le rôle des comités d'éthique

4.4.1 Le dispositif « charte et comité d'éthique »

168. Les chartes d'éthiques (qui peuvent arborer différentes dénominations) sont un moyen pour les collectivités de s'engager à aller au-delà « des obligations législatives et réglementaires qui encadrent le régime de la vidéosurveillance afin de veiller au bon usage de ce système et garantir les libertés individuelles et collectives ».

169. Dans le secteur public, certaines collectivités ont fait le choix de se doter de comités d'éthique qui ont mise en œuvre des chartes de déontologie. Sans que cela soit une obligation légale et ne résulte donc que d'une démarche volontaire de la part des collectivités, leur mise en place permet d'assurer une transparence dans la démarche et par là, une implémentation facilitée auprès de l'opinion publique.

170. En amont, elles permettent de préciser les bonnes pratiques découlant d'obligations législatives ou réglementaires ou même de combler certaines lacunes. Ces chartes posent les limites entre utilisation de la vidéoprotection à des fins d'ordre public et respect des libertés individuelles et collectives.

171. En aval, en instaurant pour la plupart un comité d'éthique, les collectivités s'assurent de l'effectivité de ces chartes. D'une part donc ces comités servent à la bonne observation des obligations imposées par la loi et les règlements (droit d'accès, obligations s'imposant aux agents chargés de visionner les images, etc.) et d'autre part, ces comités sont saisissables par n'importe lequel des citoyens qui estime avoir subi un préjudice direct et personnel découlant de la non-observation des règles.

172. De plus la plupart de ces comités peuvent formuler des observations à l'attention du Maire de la commune et doit en tout état de cause remettre un rapport annuel d'activité. Ils se positionnent donc en tant que garant des libertés collectives et individuelles tel qu'en font état les chartes.

173. En général, les chartes d'éthique rappellent les règles légales de communication et d'accès aux enregistrements ainsi que les modalités de recours en cas de refus d'accès (saisine de la Commission départementale des systèmes de vidéoprotection, des tribunaux, etc.).

174. Certaines chartes d'éthique prévoient une procédure spécifique d'exercice du droit d'accès aux images avec par exemple, la possibilité de se faire assister d'un membre du comité d'éthique ou encore d'informer ce dernier en cas de refus d'accès.

4.4.2 Tableau comparatif de quelques chartes éthique[31]

	Paris	Clichy	Lyon	Rouen	Sénart	Saint Benoît	Hayange	Communauté de commune du pays de Lure	Argenteuil
Composition du Comité d'éthique	10 membres et 1 président nommé conjointement par le Préfet de Police sur proposition du Maire de Paris	5 élus représentant à la proportionnelle les différents groupes politiques du Conseil municipal 5 suppléants 5 personnalités « orales » désignées par le Maire sur proposition du CLSPD. Le Maire de la ville est membre de droit	Elus répartis entre majorité et opposition, personnalités qualifiées représentant le monde du droit, de l'économie et de l'éducation, représentants d'associations de défense des droits de l'homme	Elus répartis entre majorité et opposition, personnalités qualifiées et d'institutions, de représentants d'associations de défense des droits de l'homme et de représentants de structures syndicales ou associatives	Président du San de la ville, le maire, le Procureur de la République près du TGI de Melun, le Bâtonnier à l'ordre des avocats du barreau de Melun Président de 'l'association d'aide aux victimes, Président du Conseil de développement de Sénart, animé par le Président du CLSPD et assisté du chef de la Circonscription de la police de Moissy-Cramayel-Sénart, un expert extérieur, la coordinatrice du CLSPD, le responsable du CSUI de Sénart.	Elus de la majorité et de l'opposition, 5 membres	4 élus représentant les différents groupes politiques du conseil municipal, 4 suppléants et des membres désignés par le Maire sachant que ce dernier est membre de droit	29 membres	7 membres représentants la majorité et l'opposition, 7 membres invités représentant la sous-préfecture, la police nationale, le conseil général, le ministère de la justice, le ministère de l'éducation nationale, Argenteuil-Bezons-Habitat et les pompiers, 7 autres membres représentent les usagers (ex : association de parents d'élèves)

[31] Liste des sites en annexe 3 du présent livre blanc.

Fréquence des sessions ordinaires	2 fois par an pour élaborer un rapport annuel public[32]	3 fois par an	Au moins 1 fois par an pour élaborer un rapport annuel	Au minimum 2 fois par an	Au moins 1 fois par an pour élaborer un rapport annuel	Au moins 1 fois par an pour élaborer un rapport annuel	Réunion d'office à la demande de son président ou à la demande justifiée d'un des membres	Non précisé	Non précisé
Information sur le droit d'accès	Rappel de la loi + possibilité de se faire accompagner d'un membre du comité d'éthique et information du comité en cas de refus d'accès	Rappel de la loi + possibilité de se faire accompagner par un membre du comité d'éthique et déferrement au tribunal administratif en cas de refus d'accès	Rappel de la loi + parmi les entités extérieures, seule la Direction départemen-tale de la sécurité publique est habilitée à demander d'observer les images	Rappel de la loi + possibilité de se faire accompagner par un membre du comité d'éthique et déferrement au tribunal administratif en cas de refus d'accès	Rappel de la loi + le visionnage en direct est organisé pendant les heures les plus criminogènes au Centre de supervision urbain intercommunal (CSUI)	Rappel de la loi + possibilité de déferrement au tribunal administratif en cas de refus d'accès	Rappel de la loi + possibilité de se faire accompagner d'un membre du comité d'éthique et déferrement au tribunal administratif en cas de refus d'accès	Rappel de la loi + possibilité de déferrement au tribunal administratif en cas de refus d'accès	Rappel de la loi + possibilité de se faire accompagner d'un membre du comité d'éthique et déferrement au tribunal administratif en cas de refus d'accès

[32] Rapports 2009 – 2010 – 2011 disponibles à l'adresse : http://www.prefecturedepolice.interieur.gouv.fr

Modalités particulières d'exercice du droit d'accès	La préfecture de Police met en œuvre le droits d'accès aux images par un numéro de téléphone dédié et une téléprocédure [33].	La demande d'accès doit être adressée au Chef de la police municipale de la ville via une fiche à remplir L'intéressé bénéficiant du droit d'accès pourra visionner les images dans un local sécurisé du poste de police municipale de la ville	Un protocole d'accès à la salle d'exploitation a été mis en place Tous les agents et opérateurs suivent une formation initiale portant sur le régime juridique de la vidéoprotec-tion, ses enjeux et les responsabilités à assumer	La demande d'accès doit être envoyée par lettre avec accusé de réception auprès du Directeur de la Police Municipale, qui doit saisir le comité d'éthique de cette demande	La demande d'accès doit être faite auprès du CSUI soit par courrier électronique, soit par appel téléphonique, soit par le site de la ville Seuls les motifs prévus dans le formulaire de réponse à la demande de consultation peuvent être invoqués pour refuser l'accès L'intéressé doit signer un récépissé de prise de connaissance des enregistrements	La demande doit être adressée au Responsable de la Police Municipale de Saint-Benoit par lettre avec accusé de réception La personne autorisée à visionner les images doit être accompagnée d'une personne habilitée	La demande doit être adressée au service juridique de la mairie de la ville Le bénéficiaire du droit d'accès peut visionner les images dans le local sécurisé du poste d'exploitation, indépendant du centre superviseur urbain	La demande doit être adressée au responsable de la police municipale de la ville via une fiche à remplir	Une convention a été signée entre la Police Nationale et la Ville afin de fixer les règles d'échange d'information et de transmission des images La demande doit être adressée par lettre avec accusé de réception au responsable de la police municipale

[33] Pour exercer son droit d'accès aux images du PVPP, un administré peut laisser un message sur la ligne téléphonique dédiée 01.40.49.70.71 ou déposer une demande par internet via le site « mon service-public.fr ».

4.5 Constats et propositions du groupe de travail

175. La personne souhaitant accéder aux images qui la concernent doit seulement justifier de son identité. Le droit d'accès à des enregistrements réalisés par un dispositif de vidéoprotection n'a pas à être motivé pour être exercé.

176. Le demandeur n'a donc pas à préciser les motifs de sa demande ou à justifier d'un quelconque préjudice pour agir.

177. Dans certaines communes, les administrés demandent un accès aux enregistrements vidéo pour retrouver un objet égaré (clés, portefeuille, etc.) ou tout simplement pour vérifier que ce droit peut être exercé.

178. Est-ce la finalité du droit d'accès aux enregistrements de vidéoprotection ?

179. La loi ne prévoit pas d'avantage de limitation en cas d'usage abusif de ce droit contrairement au droit d'accès aux traitements de données à caractère personnel encadrés par la loi Informatique et libertés.

180. L'article 39 de la loi du 6 janvier 1978 permet en effet au responsable du traitement de s'opposer « aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique ».

181. Rien de tel n'est prévu en matière d'enregistrements réalisés par un dispositif de vidéoprotection. En théorie, une demande d'accès à un enregistrement pourrait donc être faite tous les 3 mois sans qu'il soit possible d'opposer un refus.

182. En outre, seules les images concernant la personne exerçant son droit d'accès lui sont accessibles. Ce qui conduit à refuser une demande d'accès dès lors que l'on ne peut masquer ou « flouter » le visage des personnes qui ne sont pas concernées par la demande d'accès.

183. En pratique, de nombreuses demandes d'accès se trouvent ainsi refusées dès lors que la vidéo comporte l'image d'autres personnes, l'accès aux enregistrements pouvant en effet porter atteinte aux droits des tiers qui y figurent.

184. Certaines des difficultés pratiques sur la mise en œuvre du droit d'accès soulevées ci-dessus pourraient être résolues en prenant en compte les usages sur le terrain.

185.For du recul que l'on a sur l'usage du droit d'accès tel que pratiqué aujourd'hui, il devrait être possible sans remettre en cause le principe même de ce droit, de l'ajuster.

186.L'installation d'un système de vidéosurveillance est aujourd'hui clairement encadrée soit par une demande d'autorisation (lieux publics), soit par une déclaration (lieux privés). Ce dispositif totalement transparent offre une garantie aux citoyens pour le respect des libertés publiques.

187.Le responsable du système serait tout-à-fait à même d'encadrer lui-même la mise en œuvre de ce droit sur le plan pratique si la loi le permettait expressément. Elle pourrait définir son champ d'action quant à ce droit

188.De même que la réglementation impose au responsable du traitement de tenir un registre comme élément de preuve de la destruction des enregistrements dans le délai requis, elle pourrait également lui imposer de tenir un registre des demandes de droit d'accès avec les réponses fournies aux demandeurs (refus, acceptations, suites, etc.).

189.Ce registre serait une manière d'appréhender non seulement la diversité des situations mais également d'harmoniser les réponses apportées.

Propositions du groupe de travail

- Modifier le Code de la sécurité intérieur pour :
  - limiter expressément le droit d'accès aux images à un motif en rapport avec les finalités de la vidéoprotection (accident de la circulation, violence aux personnes ou aux biens, fraude au DAB, etc.).
  - sanctionner l'usage abusif du droit d'accès
- Conseiller aux établissements publics et privés disposant de systèmes de vidéoprotection de mettre en place une procédure de traitement du droit d'accès avec la tenue d'un registre des demandes et des réponses fournies.

5. Sous-groupe : Mobilité, interopérabilité, mutualisation des images, certification et sécurité

190. Pour tendre vers une plus grande efficience de la vidéoprotection dans son usage au quotidien, une réflexion semble indispensable aujourd'hui sur les questions de mobilité, d'interopérabilité, de mutualisation des images via des conventions et partenariats publics/privés, sans oublier la sécurité des réseaux.

5.1 Mobilité et définition des périmètres : les caméras piétons

191. La mobilité avec les technologies avancées (cas des drones civils) fait exploser les périmètres. Or, une caméra embarquée est traitée différemment d'une surveillance temporaire (mais fixe).

192. Aujourd'hui on trouve en vente libre sur internet de nombreux dispositifs que l'on peut installer soi-même. Or, il peut y avoir, dans certains cas, une atteinte à la vie privée.

193. Comment la loi permet-elle d'encadrer ces dispositifs ?

194. Le cas des caméras intégrées dans des drones/aéromodélismes, est révélateur : comment sont encadrés les dispositifs embarqués sur des drones utilisés hors cadre LOPPSI ?

5.1.1 Les expérimentations dans le secteur public

195. Dans le secteur public, les dispositifs mobiles et/ou embarquées sont encadrés par la LOPPSI pour les forces de l'ordre (gendarmerie, police nationale, police municipale, etc.).

196. Fixées à l'uniforme, principalement au niveau de la poitrine (plastron) à déclenchement manuel, ces caméras permettent aujourd'hui aux policiers et/ou gendarmes de filmer leurs interventions en direct, de capter toute scène, de jour comme de nuit, à l'initiative des forces de l'ordre. Il s'agit de « caméras piétons » ou encore de « caméras portatives » type Go Pro.

197. De même, de plus en plus de véhicules des forces de l'ordre sont équipés de caméras embarquées.

198. L'objectif est d'améliorer les relations entre la police et la population, sécuriser les forces de l'ordre, faire baisser des outrages, lutter contre les contrôles aux faciès ou encore fournir à l'autorité judiciaire des

précisions sur les conditions d'une interpellation. Les images et le son sont enregistrés dans une carte mémoire puis sont retranscris sur des CD-Rom, de façon à servir éventuellement de preuves, quand nécessaire.

199. La réglementation est encore à construire. Elle est fondée sur une expérimentation qui a été mise en place à l'automne 2012 dans plusieurs zones de sécurité prioritaires (ZSP), pour des fonctionnaires de police et des militaires de la gendarmerie travaillant en tenue.

200. Le ministre de l'intérieur a précisé dans une réponse ministérielle du 13 mai 2014 que cette utilisation expérimentale de caméras-piéton est pour l'heure « réservée aux seuls fonctionnaires de police et militaires de la gendarmerie nationales dans la mesure où les contrôles d'identité relèvent de leur compétence »[34].

201. Pourtant, de nombreuses communes ont déjà équipé leurs policiers municipaux de caméras portatives.

202. A la fin de l'année 2013, 238 caméras étaient affectées dans les services de police dans ces ZSP et 528 en zone gendarmerie. Le ministre de l'intérieur a précisé que :

« A l'issue de cette expérimentation, qui s'inscrit d'ores-et-déjà dans le cadre des dispositions relatives au droit au respect de la vie privée (articles 9 du code civil et 226-1 du code pénal), le cadre juridique d'emploi des « caméras-piétons » sera précisé »[35].

203. Des villes comme Nîmes, Avignon, Courcouronnes, Chelles, Saint-Denis, Saint-Étienne ou encore Poissy ont fait ce choix, en équipant en partie les agents[36].

204. Une commune, Rillieux-la-Pape, située dans la banlieue nord de Lyon, a décidé fin août 2014, de généraliser le système de caméras portatives à ses 13 policiers municipaux. Elle a constaté une baisse des outrages de 70 %. Munis de leur caméra type Go Pro, les policiers de cette commune ont l'obligation d'avertir systématiquement les personnes lorsqu'elles sont filmées et les images sont gardées 15 jours.

205. Chaque caméra enregistre les images sur une carte mémoire et les données peuvent être transférées pour visionnage « lorsque l'utilité se présente ». Une deuxième caméra équipe également l'intérieur des deux voitures de police de la ville, afin d'avoir des images « en cas de débordement ». Le maire de cette commune annonce que le parc de caméras devrait passer de 9 à 100 d'ici 2020[37].

206. Néanmoins, les collectivités territoriales s'interrogent sur les autorisations à solliciter et les textes réglementaires à respecter avant de mettre cet outil à disposition de leur police municipale. La réglementation de 1995 concerne la vidéoprotection urbaine et la vidéoprotection dans le cercle privé, notamment les commerces.

207. Cependant aucun texte ne précise pour ce type d'équipement les démarches à entreprendre auprès de la Cnil ou de la préfecture, ni la durée de sauvegarde des images, de leurs exploitations ou droit d'accès. Elles souhaitent connaître la réglementation qui s'applique aux caméras-piéton portées dans le cadre de leurs missions par les policiers municipaux.

208. Interrogé sur ces questions et les résultats du dispositif d'expérimentation de « cameras-piétons » à Nîmes, Saint-Denis ainsi qu'à Saint-Étienne, le ministre de l'intérieur a précisé que :

« S'agissant d'une expérimentation, leur doctrine d'emploi n'est pas encore fixée de manière précise et définitive. Il doit toutefois être souligné que ces caméras n'ont pas à ce stade vocation à filmer des lieux

[34] Question n° 45738, Réponse publiée au JO Ass. Nat. le 13-05-2014, p. 3898, cf annexe 4 du livre blanc.
[35] Question n° 45738, précitée.
[36] Voir : http://www.lagazettedescommunes.com/?p=226085
[37] Voir : http://www.lagazettedescommunes.com/259033/a-rillieux-la-pape-les-policiers-municipaux-equipes-de-cameras-portatives/

privés. Le cadre juridique est en effet à l'étude pour déterminer les conditions d'emploi des caméras-piéton (enregistrement de toutes les interventions ou des seules situations à risque...consentement des personnes filmées...), la nature des lieux dans lesquels un enregistrement peut être réalisé (lieu public, lieu privé ouvert ou non au public...) et la durée de conservation des données (images et sons). Un projet d'arrêté-cadre relatif au dispositif des caméras est en préparation. Un suivi régulier de l'expérimentation, à partir des retours d'expériences des utilisateurs, est assuré par un comité de pilotage réunissant au niveau central (direction générale de la police nationale) les services techniques et les services opérationnels. Cette instance s'est déjà réunie à quatre reprises. D'ores et déjà, le premier bilan d'utilisation est positif, puisque l'objectif principal est atteint : les caméras « pacifient » les relations entre les utilisateurs et les personnes contrôlées. Par ailleurs, les images et le son sont de très bonne qualité »[38].

209. Le ministre de l'intérieur a par ailleurs annoncé un projet d'arrêté-cadre relatif au dispositif des caméras en cours de préparation. Il semble néanmoins que ce projet de texte soit limité à la police nationale et à la gendarmerie.

5.1.2 Dans le secteur privé

210. Les usages de la vidéo embarquée dans le secteur privé s'étendent, alors que de nombreuses questions se posent.

- A-t-on le droit d'installer une caméra avec mémoire flash dans un véhicule pour filmer l'environnement immédiat dans le but d'apporter une preuve en cas de contestation, contravention ou accident ?
- Peut-on partager ces vidéos en ligne alors que la législation n'autorise pas à filmer la voie publique ?
- Les forces de l'ordre, la justice, les assureurs prennent-ils tout de même en compte des vidéos, en cas de preuve de litige, d'incident etc. ?
- Qui sont précisément les utilisateurs de caméras mobiles ?

211. Il ne semble pas que ce type d'usage soit interdit sous réserve du respect du droit à l'image (art. 9 C. civ. et 226-1 du C. pén.), des principes encadrant la collecte de données à caractère personnel (Cnil), du droit du travail ou encore des interceptions illégales de sécurité (écoutes téléphoniques).

212. Cependant, la Cnil, rappelle que :

« Seules les autorités publiques (les mairies notamment) peuvent filmer la voie publique. Ni les entreprises, ni les établissements publics ne peuvent filmer la voie publique. Ils peuvent seulement filmer les abords immédiats de leurs bâtiments et installations (la façade extérieure par exemple mais pas la rue en tant que telle) dans les lieux susceptibles d'être exposés à des actes de terrorisme. Les particuliers ne peuvent filmer que l'intérieur de leur propriété. Ils ne peuvent pas filmer la voie publique, y compris pour assurer la sécurité de leur véhicule garé devant leur domicile »[39].

213. Le développement de l'utilisation de robots mobiles pilotables à distance pose également des questions.

214. Le terme "robot mobile" n'est pas vraiment approprié bien que ce soit la terminologie couramment employée. Si l'équipement obéit à des éléments préprogrammés, il vaut mieux utiliser le terme d'automate que celui de robot.

215. La notion de mobilité s'évalue à deux niveaux : l'automate (la caméra) est capable d'avoir un champ d'action plus ou moins large à 360°par rapport à un point fixe et il peut se déplacer non pas sur son point fixe (caméra 360°) mais être piloté (le point fixe est déplacé). La différence est importante car si l'on veut structurer le droit, il faut d'abord structurer l'objet.

[38] Questions n° 37524 et n° 37525, Réponses publiées au JO Ass. Nat. le 11-03-2014, p. 2424, cf annexe 4 du livre blanc.
[39] Voir fiche Cnil « Vidéosurveillance - vidéoprotection sur la voie publique », juin 2012 : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_voie_publique.pdf

216. Le terme “pilotable” a également son importance. Si l’on prend le cas d’un robot domestique de télé-assistance, on peut, par exemple, faire une “levée de doute vidéo” en déplaçant la caméra par un pilotage à distance pour savoir si une personne est réellement en danger (malaise, chute, etc.), – auquel cas une intervention directe sera déclenchée — ou si elle a simplement enlevé ou débranché son appareil de contrôle.

217. Bien qu’il n’y ait pas de cadre juridique spécifique pour ce type d’usage en France, ces robots mobiles pilotables à distance sont néanmoins soumis aux mêmes contraintes réglementaires que les systèmes de vidéoprotection (notamment le masquage des zones privées) car ils peuvent capter et diffuser des données personnelles.

5.2 Mobilité et définition des périmètres : les caméras embarquées

5.2.1 Les caméras embarquées dans les transports en commun

218. Les équipements de systèmes de captages d’images de vidéoprotection à bord de matériels roulants (Trains, Tramways, Bus) sont des options retenues par les Activités de transport public de voyageurs et par l’Autorité Organisatrice territorialement compétente, afin de contribuer à limiter les faits d’incivilité et les actes de malveillance et à diminuer le sentiment d’insécurité.

219. Ce choix a donc pour finalités la sécurité des personnes, la prévention des atteintes aux biens et aux actes terroristes.

220. Ces équipements de systèmes de captages d’images de vidéoprotection embarquée sont régis par les mêmes dispositions législatives et réglementaires qu’un dispositif de même nature installé sur un site ou un établissement recevant du public : Déclaration préfectorale, signalétique, personnel désigné et dûment habilité, traçabilité (registres), destruction des images dans le délai légal, normes techniques, droit personnel d’accès aux enregistrements etc.

221. La particularité du dispositif législatif réside au niveau des systèmes pluri départementaux : la Préfecture compétente, pour la demande d’autorisation, est celle du département du siège de l’entreprise de transport public de voyageurs.

222. Au même titre qu’un système vidéoprotection installé dans un établissement recevant du public, ces dispositifs peuvent faire l’objet de réquisitions d’images émanant des autorités judiciaires, dans le cadre d’une enquête consécutive à un événement relevant de la sûreté à bord.

223. Dans de nombreuses agglomérations de province, les transporteurs ont équipé leur réseau de caméras embarquées, à l’instar de Transpole à Lille et de Keolis à Lyon. La communauté urbaine de Lille a mis en place la vidéo-protection embarquée dans toutes les rames du métro pour visionner en direct l’intérieur des rames, depuis le poste de commande centralisée (PCC), et déclencher l’intervention du personnel de Transpole Lille ou des forces de l’ordre en cas d’incident[40].

224. C’est également le cas de la communauté d’agglomération de La Rochelle qui a financé début 2014, l’installation de caméras dans 50 des 80 bus de la flotte locale. La liste des villes équipées partiellement ou totalement en matériel de vidéo-surveillance embarquée ne cesse de croître.

[40] Voir : http://www.lillemetropole.fr/files/live/sites/lmcu/files/docs/TRANSPORTS/Plaquette-nouvelle-ligne1_mai2013.pdf

225. En Ile de France, la vidéoprotection est déployée sur l'ensemble du réseau RATP, ce qui représentait en 2012, 8750 caméras sur les espaces du réseau ferré, 18 000 caméras embarquées à bord des bus. Le nouveau matériel roulant (rames et trains) en est également équipé[41].

226. Dans les dispositifs de vidéo-protection embarquée, l'enregistrement vidéo peut être soit être continu, soit à la demande du chauffeur. Les données sont sauvegardées dans le bus pour une durée moyenne variable selon les systèmes (de quelques heures à quelques jours). Les bandes vidéo sont visionnées, par des personnes assermentées, uniquement en cas d'incidents, sinon, elles sont réutilisées.

227. Selon les fonctionnalités retenues, les systèmes de vidéo-surveillance embarquée peuvent être interconnectés avec la transmission radio, permettant ainsi au régulateur d'entendre ce qui se passe dans le véhicule, et même de transmettre le son aux forces de l'ordre.

228. L'intérêt de ces systèmes est acquis pour ce type d'espace, les enregistrements permettant notamment au service sécurité des entreprises de transport de travailler avec les services de la police et de la justice, par exemple dans le cadre des contrats locaux de sécurité.

5.2.2 Les caméras embarquées sur les drones

229. L'usage des drones est de plus en plus développé du fait d'une plus grande accessibilité de cette technologie tant par le grand public que les professionnels. Pour une majorité d'entre ces derniers, l'intérêt des drones est sans appel du fait de leur capacité à protéger et surveiller via une caméra embarquée.

230.Il convient de distinguer les drones à usage professionnel des drones de loisirs « aéromodèle »

5.2.2.1La distinction drone et aéromodélisme

231. Selon l'article 3 de l'arrêté du 11 avril 2012, un « aéromodèle » est un « aéronef télépiloté » utilisé exclusivement à des fins de loisirs ou de compétition par un « télépilote » toujours capable d'en conserver le contrôle. Les engins ne comportant ni caméra ni appareil photo embarqué sont classés en « catégorie A », c'est-à-dire pesant moins de 25 kg au décollage (masse structurale et charge emportée) et à gaz inerte, moteur électrique ou turbopropulseur d'une puissance inférieure ou égale à 15 kW (art. 4 de l'arrêté)[42].

232. A condition de ne pas dépasser les hauteurs maximales de vol prescrites par la réglementation (150 mètres), les drones d'aéromodélisme de catégorie A sont dispensés de « document de navigabilité » et sont « autorisé à voler sans autre condition relative à leur aptitude au vol et sans autre condition requise des personnes qui les utilisent » (Annexe I, 1.1 de l'arrêté).

233. Néanmoins, un second arrêté du 11 avril 2012, indique que le vol à vue directe d'un aéromodèle de loisirs, hors zone peuplée, est autorisé « sous réserve qu'il n'en résulte pas un risque manifeste de dommage à autrui » (art. 4 de l'arrêté, § 4.1).

234. La DGAC s'est positionnée par écrit en avril 2014[43] sur le site du Ministère en spécifiant qu'il y a une différence entre les drones et les aéromodèles y compris équipés de matériel de prise de vue.

235. Un aéromodèle ne peut-être qu'utilisé qu'en loisir ou compétition et n'entrera pas en activité spéciale lors de prise de vue à titre privé.

[41] IAU (Institut d'aménagement et d'urbanisme de l'Ile de France), Note rapide N° 603 - août 2012, www.iau-idf.fr
[42] Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent (NOR: DEVA1206042A).
[43] « Drones civils : loisir ? aéromodélisme ? activité professionnelle ? », 30 avril 2014, http://www.developpement-durable.gouv.fr/Drones-civils-loisir-aeromodelisme

236. La DGAC rappelle que l'arrêté du 11 avril 2012 relatif aux conditions d'emploi des aéronefs télépilotés fait une distinction claire entre ceux qui sont utilisées pour le loisir et la compétition (les aéromodèles) et les autres.

237. Lorsque la prise de vue est accessoire à un vol de loisir ou de compétition, et que les images ne sont pas exploitées après le vol à des fins professionnelles, commerciales publicitaires ou autres que privées, elle ne rentre pas dans la catégorie des activités particulières, et elle peut être faite par un aéromodéliste.

238. Il convient de rappeler à cet égard que comme les autres aéronefs télépilotés, les aéromodèles sont soumis au 2ème arrêté du 11 avril 2012, relatif à l'espace aérien qui stipule entre autres que sauf autorisation particulière, le survol des agglomérations et des rassemblements de personnes est interdit et donc également la prise d'images dans ces conditions.

5.2.2.2 Les expérimentations

239. La SNCF Infrastructure a commencé, fin 2013, certaines expérimentations avec des drones : pour inspecter les voies, les parois rocheuses escarpées, surveiller les caténaires, détecter d'éventuels obstacles sur la voie en cas d'intempéries, repérer tout acte de malveillance dans des zones rendues difficiles d'accès par la route, vérifier le bon fonctionnement des réchauffeurs d'aiguilles en hiver, etc.[44]

240. Elle expérimente également l'utilisation de drones dans des zones urbanisées notamment pour lutter contre le phénomène des vols de câbles de cuivre sur les voies ferrées et autres actes de vandalisme. Une expérimentation est en cours dans la région Midi-Pyrénées pour vérifier la faisabilité d'une surveillance de nuit des infrastructures ferroviaires en zones peu habitées.

241. Il est encore trop tôt pour dire ce que ce type d'expérimentation va donner ni les évolutions réglementaires que la DGAC sera éventuellement amenée à faire. Interviewé en février dernier, le ministre des Transports Frédéric Cuvillier a souligné, que l'utilisation des drones en complémentarité avec d'autres moyens, tels les hélicoptères de la gendarmerie, pourrait être « une bonne idée », tout comme la possession, à terme, « d'une escadrille »[45].

242. Pour chaque expérimentation de drone, une demande d'autorisation de vol à la Direction générale de l'aviation civile (DGAC) est obligatoire. La réglementation française prévoit plusieurs scénarii qui vont du vol en vue directe du pilote avec des drones pesant plusieurs dizaines de kilos, aux missions hors vue de drones d'un poids de moins de deux kilos.

243. La SNCF, EDF et la DGAC œuvrent ensemble pour participer au développement de cette nouvelle filière industrielle française ; ce qui devrait nécessiter quelques évolutions législatives.

244. Lors des récentes inondations qui ont touché le sud de la France, en janvier 2014, un drone a apporté un appui visuel précieux aux secours au sol, afin de localiser les zones les critiques et les potentielles victimes.

245. La DGCA a mis en ligne les démarches pour effectuer des activités particulières et des expérimentations avec un drone (aéronef télépiloté)[46].

[44] « Innovation, la SNCF teste des drones pour inspecter les ouvrages d'art », brochure disponible sur http://www.sncf.com/ressources/dp_drones.pdf

[45] Cf. Stéphane Volant, « La SNCF va expérimenter l'utilisation de drones dans des zones urbanisées », AEF Sécurité globale, février 2014.

[46] Démarches pour effectuer des activités particulières et des expérimentations avec un drone (aéronef télépiloté), 10 mars 2014 (mis à jour le 15 mai 2014), http://www.developpement-durable.gouv.fr/Demarches-pour-effectuer-des.html

5.2.2.3 La règlementation des drones à usage civil

246. L'arrêté ministériel qui fixe les conditions de développement du secteur des drones à usage civil date d'avril 2012.

247. Sur le marché civil, la nouvelle réglementation de la DGAC (direction générale de l'aviation civile) semble assez contraignante, du point de vue des industriels du secteur développant ces produits. Ainsi, le Président de Bertin Technologies déplore *"On ne peut pas faire voler un drone à plus d'1 km de la station de contrôle"*.

248. Sur le marché des drones étatiques, selon toujours le même dirigeant, les règles imposées par la DGA (Direction générale de l'armement) ne favorisent pas le développement de ce marché.

249. Les limites fixées par les arrêtés du 11 avril 2012 sont en effet très contraignantes[47]. Dès qu'ils sont équipés d'un dispositif de prise de vues (appareil photo, caméra de type GoPro) et qu'ils effectuent des « activités particulières », les drones sont considérés comme effectuant un travail aérien, soumis à l'autorisation de la DGAC. Il y a de nombreuses règles à respecter du fait de son insertion dans l'espace aérien civil réglementé par la DGAC[48].

250. Le texte qui précise la réglementation applicable aux « aéronefs civils qui circulent sans aucune personne à bord » (drones) est l'arrêté du 11 avril 2012 pris par le ministre chargé de l'aviation civile.

251. Il réglemente leur conception et conditions d'emploi ainsi que les capacités des personnes qui les utilisent. L'arrêté répertorie les drones par catégories liées essentiellement aux poids (« masse structurale » et « charge emportée ») et systèmes de propulsion (moteur thermique, électrique, à gaz inerte, etc.). Au total, 7 catégories sont définies (A à G)[49].

252. Mais l'arrêté ne se limite pas aux seuls critères du poids et du mode de propulsion pour autoriser les vols de drones. Il tient compte également du rayon d'action, de la hauteur de vol, des conditions de circulation (vol à vue ou hors vue du pilote) et surtout de la zone survolée.

253. L'arrêté permet ainsi l'utilisation de drones pour des activités aériennes prédéfinies suivant 4 scénarios d'usages. C'est en fonction de sa catégorie et du scénario d'usage que l'utilisation d'un drone est subordonnée :

- à l'obtention du certificat de navigabilité (CDN) délivré par la DGAC, valant autorisation de vol ;
- au dépôt d'un dossier MAP (Manuel d'activité particulière) à la DGAC et d'une déclaration de conformité à la réglementation ;
- à une formation spécifique de télépilote et une déclaration de niveau de compétence (DNC).

254. D'autre part, le drone doit disposer de toutes les mesures permettant d'assurer la sécurité des tiers et décrites dans l'arrêté du 11 avril 2012 (traitement des pannes et des pertes de contrôle, limitation des risques en cas d'impact, gestion « contrôlée » du crash en cas de perte de contrôle, etc.).

255. Même utilisé à des fins professionnelles par des opérateurs privés habilités, un drone civil ne peut survoler de zones habitées (dites « zones urbanisées »). Un arrêté du 24 décembre 2013 ne prévoit cette possibilité que pour des drones appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile.

[47] Arrêtés du 11 avril 2012 (NOR: DEVA1207595A) et (NOR: DEVA1206042A).
[48] Alain Bensoussan, « Drones légaux : le début de l'usage civil », Planète Robots n°26, mars-avril 2014.
[49] Arrêté du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord (NOR: DEVA1207595A).

5.2.2.4 Les règles de sécurité

256. Le Service d'information et de relations publiques des armées et de la gendarmerie (SIRPA) signale le cas d'un individu ayant fabriqué un drone de type hexacoptère et qui a survolé Paris et le quartier de La Défense en filmant des images qu'il a posté sur internet pour « faire le buzz »[50]. Convoqué en février 2014 par la brigade de la gendarmerie des transports aériens d'Issy-les-Moulineaux, il a reconnu les faits dont plusieurs survols de Paris, la violation de l'article L6232-4 du Code des transports (vol d'un aéronef sans obtention d'un document de navigabilité)[51] et de l'article L39-1 du Code des postes et des communications électroniques (utilisation de fréquences radioélectriques sans autorisation)[52].

257.De même, une autre affaire a aboutie à la condamnation d'un jeune militaire, à une amende de 500 euros pour « conduite d'un aéronef non-conforme aux règles de sécurité » après avoir fait voler un drone près de la Tour Eiffel[53].

258. D'autres procédures similaires ont été ouvertes par la brigade de gendarmerie des transports aériens (BGTA) de Pau-Uzein. L'une d'elle a donné lieu à la condamnation d'un professionnel de l'événementiel à une amende de 350 euros et trois contraventions de 35 euros pour avoir fait survoler le Palais Beaumont, situé en centre-ville de Pau, par un drone équipé d'une caméra et pris des images d'une manifestation publique ; malgré l'autorisation de l'établissement, il ne détenait pas l'homologation légale[54].

5.2.2.5 Les prises de vue aériennes

259. Les prises de vues et vidéos aériennes sont encadrées par l'article D133-10 du Code de l'aviation civile qui impose que « toute personne qui souhaite réaliser des enregistrements d'images ou de données dans le champ du spectre visible au-dessus du territoire national est tenue de souscrire une déclaration au plus tard quinze jours avant la date ou le début de période prévue pour l'opération envisagée auprès du chef du service territorial de l'aviation civile dont relève son domicile ».

260. En conséquence, si le vol est destiné à la prise de vues, même pour les loisirs, il doit faire l'objet d'une déclaration.

5.2.2.6 Les bandes de fréquence et la transmission des images vidéo

261. L'équipement de transmission des images vidéo doit être conforme aux décisions de l'Arcep relatives aux puissances d'émission de la réglementation en vigueur.

262. Les dispositifs ne doivent pas causer de brouillage préjudiciable aux stations d'un service bénéficiant d'une attribution à titre primaire ou secondaire dans le tableau national de répartition des bandes de fréquences. Ils ne peuvent pas prétendre à la protection contre les brouillages préjudiciables causés par ces stations.

5.2.2.7 L'usage de l'espace aérien

263. Au-delà de 150 mètres de hauteur, le drone évolue dans un espace dit « ségrégué », c'est-à-dire soumis à une autorisation spéciale avec plan de vol. Il nécessite une autorisation de vol obtenue à la suite du dépôt d'un dossier prouvant que le modèle est sûr et dispose des systèmes de sécurité adéquats.

[50] « Île-de-France, Haro sur les drones ! », Sirpa Gendarmerie, février 2014.
[51] Sanctions pouvant atteindre cinq ans d'emprisonnement et 75 000 euros d'amende.
[52] Sanctions pouvant atteindre six mois d'emprisonnement et 30 000 euros d'amende.
[53] « Les drones plus nombreux dans les airs et sur les écrans radar de la justice », La Dépêche.fr du 14 mars 2014, d'après dépêche AFP.
[54] « Les drones non homologués déjà sanctionnés en Béarn », La République des Pyrénées.fr du 17 février 2014.

264. Le non-respect de cette réglementation peut constituer une entrave à la navigation ou à la circulation aérienne, sévèrement punie par la loi. Les sanctions peuvent, selon les cas, atteindre jusqu'à cinq ans d'emprisonnement et 18 000 euros d'amende[55].

265. Des procédures sont déjà en cours[56]. Le parquet de Bayonne a notamment ouvert une enquête sur la présence d'un drone, qui pourrait avoir gêné les opérations de secours de l'équipage du cargo espagnol « Luno », échoué début février à Anglet (Pyrénées-Atlantiques). Selon une dépêche AFP du 14 mars 2014, « le pilote de l'hélicoptère militaire a été gêné par la présence d'un drone » qui aurait retardé un décollage, « à un moment où il fallait opérer au plus vite ». Le drone aurait dû avoir l'aval de la tour de contrôle de Biarritz pour se trouver dans cet espace aérien.

266. Entrent également en ligne de compte d'autres législations tout aussi importantes, telles que la mise en danger de la vie d'autrui, ou encore la protection de la vie privée.

5.2.2.8 La protection de la vie privée

267. Même si un cadre juridique et éthique reste à définir, ces robots aériens sont soumis aux mêmes contraintes réglementaires que les systèmes de vidéosurveillance[57].

268. L'usage de drones équipés d'un appareil photo ou d'une caméra doit tenir compte de la loi Informatique, fichiers et libertés encadrant le traitement des données personnelles et de l'article 9 du Code civil sur le respect de la vie privée.

269. Le respect de cette législation implique comme en matière de vidéoprotection, l'interdiction de pointer des caméras vers l'habitation ou l'entrée d'un tiers. En outre, l'utilisation de drones équipés de caméras ne doit permettre de réaliser que des prises de vues strictement limitées aux espaces extérieurs des propriétés (hors voie publique), sauf à recourir à un moyen technique de floutage automatique des zones privées.

270. La Cnil s'intéresse aux engins volants bardés de capteurs, qui peuvent être de formidables machines à observer, à emmagasiner et à analyser des données à caractère personnel. Elle a consacré en décembre 2013, un numéro spécial intitulé « Drones, innovations, vie privée et libertés individuelles » dans lequel elle s'interroge sur ces nouvelles formes possibles de surveillance des comportements et des déplacements de chacun, et plus généralement de la vie privée[58].

271. Selon la Cnil, le cadre de régulation à créer « doit à la fois tracer des lignes rouges et offrir un espace de liberté aux innovations (…). La réflexion doit être pluridisciplinaire et impliquer l'ensemble des acteurs concernés parmi lesquels les industriels du secteur, les autorités en charge de la réglementation aérienne, la société civile ».

272. La Cnil souligne par ailleurs que sa démarche est une première esquisse de la problématique autrement plus large de l'éthique de la robotique. Les réflexions de la Cnil pourraient donc aboutir à de prochaines recommandations en ce domaine.

5.2.2.9 La mise en danger d'autrui

273. Les drones ne doivent pas constituer un risque pour autrui. La qualification de mise en danger d'autrui, prévue à l'article 223-1 du Code pénal, incrimine « le fait d'exposer directement autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente par la violation manifestement délibérée d'une obligation particulière de sécurité ou de prudence prévue par la loi ou le règlement ».

[55] Code des transports, art. L6372-4.
[56] Alain Bensoussan, « Les drones devant les tribunaux », Planète Robots n°27, mai-juin 2014.
[57] Isabelle Pottier, « Drones ou robots aériens : un cadre juridique et éthique à définir », Post du 19 avril 2013.
[58] La lettre innovation et prospective de la Cnil n°06, décembre 2013.

274. Dans l'enquête précitée menée par le parquet de Bayonne sur le drone gêneur, l'infraction à la législation aérienne est également doublée d'une possible mise en danger délibérée d'autrui compte-tenue de la gêne qui a pu être occasionnée.

275. Les sanctions peuvent, selon les cas, atteindre jusqu'à un an d'emprisonnement et 15 000 euros d'amende. Mais pour que le délit soit constitué, il faut que le manquement ait été la cause directe et immédiate d'un risque de mort ou de blessures auquel a été exposé autrui et que le lien direct de causalité soit caractérisé.

276. En ce qui concerne les drones, il y aura sans doute matière à débattre, notamment lorsque l'on sera en présence de drones équipés de dispositifs de sécurité (antichute, freinage, atterrissage automatique, etc.) ou encore de drones ultra légers, non contondants et constitués de matériaux souples.

5.3 Interopérabilité, mutualisation des images (CSU/PC sécurité) et partage des compétences

5.3.1 La mutualisation des images

277. L'analyse du référentiel légal met en avant les limitations de la réglementation actuelle. Les blocages réglementaires aboutissent à multiplier les centres de supervision urbains (CSU) intercommunaux, faute de pouvoir partager les images.

278. Outre les questions de coûts, cela pose également la question de l'efficacité des dispositifs. Le renvoi des images à l'ensemble de l'intercommunalité et aux forces de l'ordre permettrait une intervention plus rapide et plus efficace en cas de commission d'un délit (agression, vol, etc.). Il y a sans doute des compromis possibles sur la mutualisation des images.

5.3.1.1 Les difficultés liées à la mutualisation des images entre public et privé

279. Dans le cadre notamment du «plan de vidéoprotection pour Paris » (PVPP), baptisé «plan 1000 caméras», la surveillance des abords immédiats des commerces, bureaux (exemple en Plaine-Saint-Denis) est difficile à mettre en œuvre notamment du fait des paramétrages pour flouter l'intérieur des bâtiments privés.

280. En outre il n'y a aujourd'hui aucune possibilité de visionner toutes les images d'une zone donnée qu'elles soient d'origine publique ou privé, et de le faire faire par des agents publics ou privés (principe de maillage et de mutualisation).

281. En mars 2011, lors de l'examen de constitutionnalité de la Loppsi 2[59], le Conseil constitutionnel a censuré l'une des dispositions visant à permettre des systèmes de vidéoprotection publique avec visionnage des images par des agents d'opérateurs privés[60].

282. Cette disposition aurait permis d'une part, d'assouplir la mise en œuvre de dispositifs de vidéoprotection par des personnes morales de droit privé et d'autre part, de déléguer à des personnes privées l'exploitation et le visionnage de la vidéoprotection.

283. Telle n'a pas été la position du Conseil constitutionnel qui a jugé que cet assouplissement permettait de confier à des personnes privées la surveillance générale de la voie publique et ainsi de leur déléguer des compétences de police administrative générale inhérentes à l'exercice de la « force publique ».

[59] Loi 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure : JO du 15 mars 2011, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id
[60] Décision CC 2011-625 DC du 10 mars 2011, www.conseil-constitutionnel.fr/decision/2011/2011625dc.htm

284. Il a jugé que des fonctions « régaliennes » comme la surveillance générale de la voie publique, ne pouvaient pas être déléguées par la loi à des personnes privées. Ces dispositions méconnaitraient l'exigence, résultant de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789, selon lequel la garantie des droits est assurée par une « force publique ».

285. Pourtant, il est intéressant de noter que cette question n'a pas été soulevée lors de la mise en œuvre en 2006, du dispositif du placement sous surveillance électronique mobile (PSEM) -plus connu sous le nom de bracelet électronique mobile-, des délinquants et criminels récidivistes les plus dangereux, alors même que la fonction de surveillance a été « privatisée »[61].

286. Le contrôle du dispositif du bracelet électronique mobile est en effet confié à une société privée, la société ElmoTech, habilitée par arrêté du 23 août 2007, au titre de l'article R. 61-36 du Code de procédure pénale, à se voir confier par contrat « les prestations techniques détachables des fonctions de souveraineté concernant la mise en œuvre du placement sous surveillance électronique mobile »[62].

287. En l'espèce, un arrêté du 23 août 2007[63] homologue le procédé technique de surveillance électronique mobile qui permet de localiser grâce à un système satellite (GPS) les personnes condamnées et placées sous surveillance électronique mobile.

288. Les mouvements du sujet peuvent être suivis en temps réel grâce à un système GPS de positionnement par satellite ; en cas de non-respect des zones, la société privée prévient l'administration pénitentiaire. Or c'est bien l'administration pénitentiaire qui est censée assurer les fonctions régaliennes de surveillance...

289. Si le fait que des personnes privées puissent visionner les zones publiques n'est pas possible, il serait peut-être souhaitable que les forces de l'ordre puissent visionner les images en zone privée car ceci s'avère très utile pour les levées de doute, notamment.

5.3.1.2 Les difficultés liées à la mutualisation CSU et PC des bailleurs sociaux

290. La réflexion porte sur l'éventuel intérêt d'assouplir ou non les règles permettant le renvoi des images aux centres de supervision.

291. Les collectivités sont de plus en plus sollicitées par les bailleurs sociaux et les copropriétaires pour un raccordement de leur réseau de caméras privées au centre de supervision urbain (CSU) communal ou intercommunal.

292. Et si les bailleurs sociaux ont rapidement confié la sécurité de leur patrimoine à une société privée de gardiennage, plusieurs d'entre elles en sont peu satisfaites. Dans certaines villes, les forces de l'ordre ont même confié n'être que très rarement alertées par les vidéo-opérateurs, lors d'une infraction perpétrée dans les espaces vidéoprotégés (halls, parkings), des bailleurs.

293. Depuis la promulgation de la Loppsi 2[64], les bailleurs ont aujourd'hui la possibilité de transmettre aux forces de l'ordre ou aux CSU de la police municipale des images émanant des caméras situées dans les parties communes des immeubles (halls, parkings), « lors de circonstances faisant redouter la commission imminente d'une atteinte grave aux biens ou aux personnes ».

[61] Le placement sous surveillance électronique, http://www.justice.gouv.fr/prison-et-reinsertion-10036/la-vie-hors-detention-10040/le-placement-sous-surveillance-electronique-11997.html
[62] Arrêté du 23 août 2007 : JO du 12 septembre 2007.
[63] Arrêté du 23 août 2007 disponible sur : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000823271
[64] Loi 2011-267 du 14 mars 2011, art. 23 insérant un article L. 126-1-1 au Code de la construction et de l'habitation.

294. Cette transmission s'effectue en temps réel et est strictement limitée au temps nécessaire à l'intervention des services de la police ou de la gendarmerie nationale ou, le cas échéant, des agents de la police municipale.

295. Une convention doit être conclue entre le préfet, le gestionnaire de l'immeuble (logement social) ou le syndic et le maire pour préciser les conditions et les modalités du transfert des images. Les modalités de cette convention sont fixées par le décret n° 2012-112 du 27 janvier 2012[65].

296.La convention doit notamment indiquer le destinataire des images, la nature du risque encouru, les modalités de transmission et de conservation des images et les conditions d'information du public.

297. La transmission des images s'effectue en temps réel et est strictement limitée au temps nécessaire à l'intervention des services de police ou de gendarmerie.

En ce qui concerne les dispositifs installés par les commerçants pour lutter contre le vol : seuls les responsables de la sécurité, les agents de sécurité ou la direction du magasin peuvent visualiser les images

298. Quelques collectivités ont créé un deuxième CSU à destination des bailleurs. Le transfert des images, autorisé dans les cas précédemment cités, est alors plus aisé.

299. De nombreux bailleurs mettent également en avant le fait qu'un renvoi des images à la collectivité, l'intercommunalité et aux forces de l'ordre favorise une intervention plus rapide et efficace.

300. Cependant, si mutualiser les images apparaît de plus en plus comme une évidence, le droit ne le permet pas, aujourd'hui.

5.3.2 L'interopérabilité des systèmes

301. Une installation de vidéo protection est un système complexe, mettant en jeu des technologies variées, dont le seul commun dénominateur est le réseau IP. Les protocoles de communication entre les caméras et les équipements périphériques, les algorithmes de compression, la gestion des métadonnées sont propres à chaque constructeur.

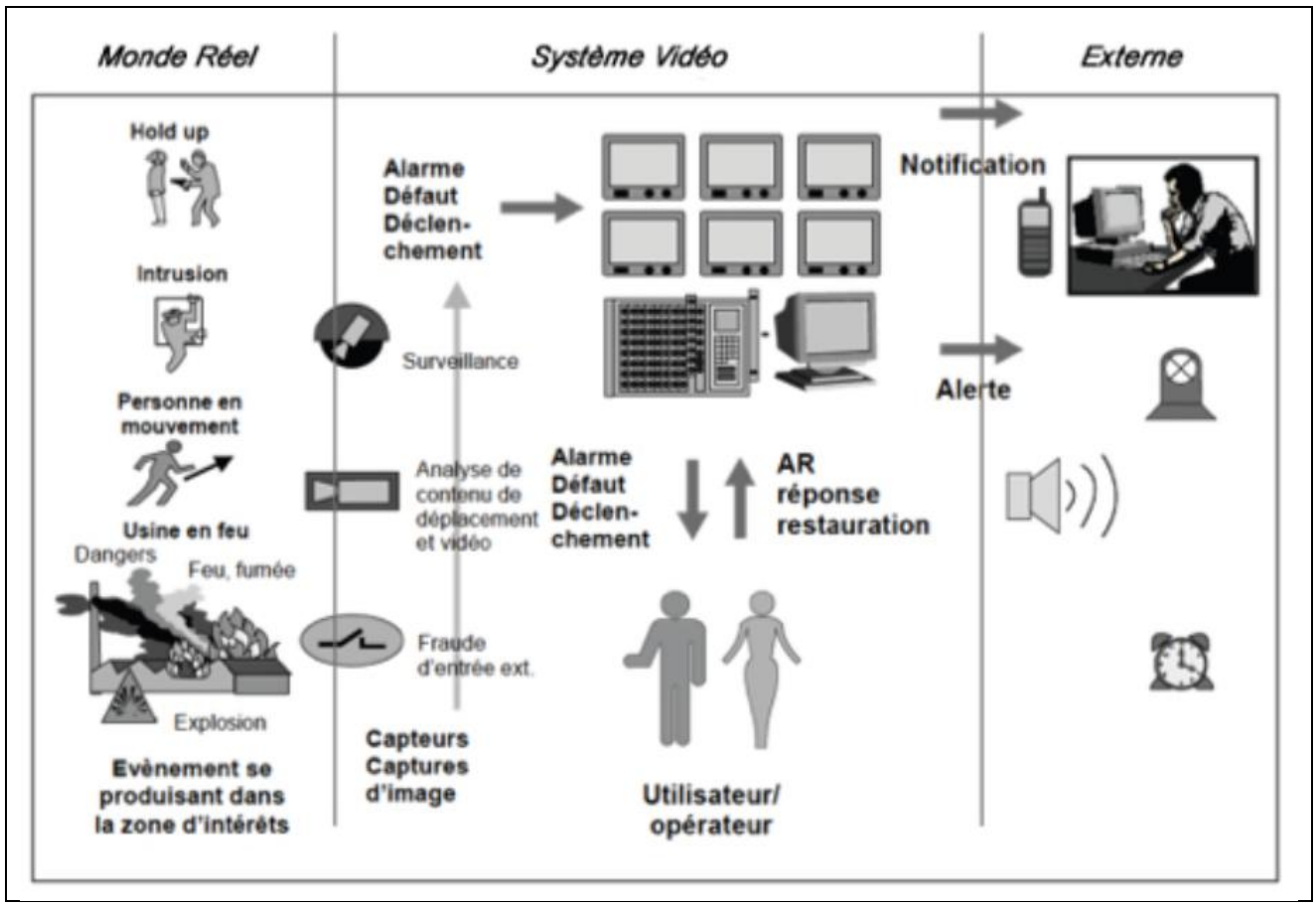
302. De plus, la migration rapide des technologies analogiques vers le numérique fait intervenir des contraintes purement liées à la gestion d'un système informatique. Or l'interopérabilité en vidéoprotection est indispensable[66].

303. L'interopérabilité au sens applicatif, traitée dans la brique fonctionnelle « Interface avec d'autres systèmes », fait partie des préoccupations du Forum Open-IPVideo, qui lui a consacré un guide en avril 2014.

304. Selon l'association réunissant des professionnels de l'écosystème de la vidéo gestion, un système de sécurité doit permettre de faire interagir la vidéo avec des systèmes de contrôle d'accès, d'intrusion ou autres.

[65] Décret 2012-112 du 27 janvier 2012, JO du 29 janvier 2014, disponible sur : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025209001&dateTexte=&categorieLien=id

[66] Conférence du Forum Open-IPVideo, « L'interopérabilité en vidéoprotection : gage de pérennité et d'efficacité », Lyon 2011, http://www.preventica.com/docs/conferences-lyon-2011/open-ip-video-interoperabilite-videoprotection.pdf



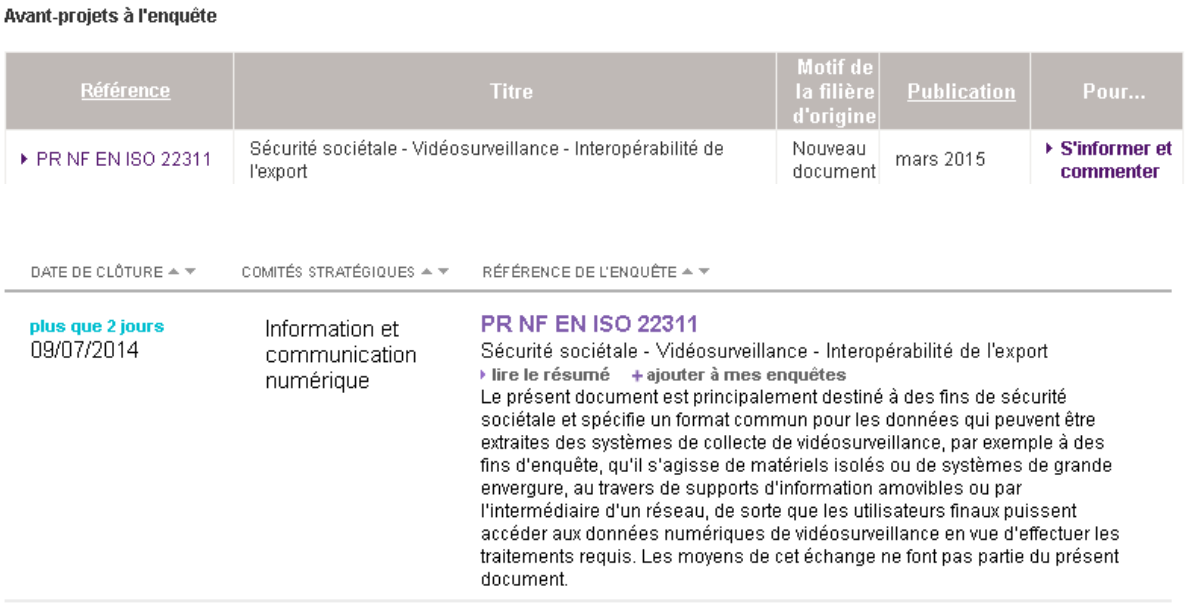
Extrait du Guide d'interopérabilité - Version 4 - avril 2014, reproduit avec l'aimable autorisation du Forum Open-IPVideo, info@open-ipvideo.org © Garry Goldenberg-Korn.

305. Dans son analyse du jeune marché de l'industrie de la vidéoprotection en réseau (années 90), le Forum Open-IPVideo constate que si les composants individuels d'un système peuvent être soumis à la conformité à des normes ou standards techniques, la réalisation et la mise en œuvre d'un système ne s'appuient actuellement que sur des normes règlementaires[67].

306. Il n'existe encore ni norme ni standard définissant l'interopérabilité entre les différents composants de la chaîne, même si les organisations internationales ont créé des groupes de travail pour l'élaboration de telles normes (AFNOR, ISO, CEI, etc.).

[67] Guide d'interopérabilité - Version 4 - avril 2014, Forum Open-IPVideo, info@open-ipvideo.org © Garry Goldenberg-Korn.

5.3.3 L'absence de norme d'interopérabilité des systèmes



Avant-projets à l'enquête

Référence	Titre	Motif de la filière d'origine	Publication	Pour...
PR NF EN ISO 22311	Sécurité sociétale - Vidéosurveillance - Interopérabilité de l'export	Nouveau document	mars 2015	S'informer et commenter

DATE DE CLÔTURE	COMITÉS STRATÉGIQUES	RÉFÉRENCE DE L'ENQUÊTE
plus que 2 jours 09/07/2014	Information et communication numérique	**PR NF EN ISO 22311** Sécurité sociétale - Vidéosurveillance - Interopérabilité de l'export lire le résumé + ajouter à mes enquêtes Le présent document est principalement destiné à des fins de sécurité sociétale et spécifie un format commun pour les données qui peuvent être extraites des systèmes de collecte de vidéosurveillance, par exemple à des fins d'enquête, qu'il s'agisse de matériels isolés ou de systèmes de grande envergure, au travers de supports d'information amovibles ou par l'intermédiaire d'un réseau, de sorte que les utilisateurs finaux puissent accéder aux données numériques de vidéosurveillance en vue d'effectuer les traitements requis. Les moyens de cet échange ne font pas partie du présent document.

Capture d'écran 1 : Enquête publique AFNOR pour l'élaboration d'une norme sur l'opérabilité des systèmes de vidéoprotection

307. Dans le cadre de certains événements, notamment liés à l'ordre public, il faudrait rendre les dispositifs interopérables (utilisation simultanée des caméras de la ville, des transports publics, du centre commercial, du stade de football, etc.). Ceci permettrait leur suivi sans rupture d'images. Cette interopérabilité demeure toutefois très théorique, les systèmes vidéo étant tellement différents qu'il est souvent difficile de les connecter les uns aux autres.

308. Finalement l'arrêté du 3 août 2007 est le seul outil à définir les caractéristiques technologiques des systèmes, que cela concerne le potentiel des caméras en matière de capture d'images, celui des systèmes d'enregistrement ou encore celui des réseaux de transmission des images.

309. Seule une norme de vidéoprotection permettrait de définir des conditions d'interopérabilité.

310. L'arrêté du 3 août ne définit que des caractéristiques fonctionnelles, et en aucun cas des conditions d'interopérabilité.

311. La seule norme publiée dans ce sens, à notre connaissance, est la norme ISO 22311, principalement destinée à des fins de « sécurité sociétale » par exemple, pour faciliter le travail d'enquête des forces de l'ordre et de la justice. Elle spécifie un format commun pour les données qui peuvent être extraites des systèmes de collecte de vidéosurveillance, par exemple à des fins d'enquête, qu'il s'agisse de matériels isolés ou de systèmes de grande envergure, au travers de supports d'information amovibles ou par l'intermédiaire d'un réseau, de sorte que les utilisateurs finaux puissent accéder aux données numériques de vidéosurveillance en vue d'effectuer les traitements requis. Cette norme n'a été publiée qu'en mars 2013[68], et n'est encore implémentée par aucun constructeur.

312. Des chercheurs ont ainsi présenté la norme ISO 2231 à la 7ème édition Workshop Interdisciplinaire sur la Sécurité Globale (WISG) 2013 :

[68] Norme NF ISO 22311 Mars 2013, Sécurité sociétale - Vidéosurveillance - Interopérabilité de l'export.

« La norme propose d'archiver les données de manière hiérarchique dans des fichiers, dossiers et groupes de dossiers. Le rangement en fichiers et dossiers est fait conformément à des créneaux temporels de répertoire (DTS) et créneaux temporels de fichiers (FTS) (le temps est donné en temps universel coordonné (UTC)). Chaque fichier contient des données (audio/vidéo) provenant de plusieurs sources (cameras), un index par contenu (audio/vidéo) permettant l'accès précis à toute image et toute heure spécifiques et des métadonnées pour chaque source (caméra) et dossier. La norme n'a pas comme objectif de définir des nouveaux modèles de métadonnées mais plutôt de proposer une structure de format d'encapsulation qui se base sur des standards déjà existants, notamment MPEG, JPEG, CEI/TC et SMPTE. Les éléments qui doivent obligatoirement être fournis par tous les systèmes de vidéosurveillance afin d'assurer un minimum d'interopérabilité (visualisation des vidéos) sont : nom et profil du codec, nom du conteneur, résolution vidéo, nombre d'images vidéo (en images/secondes), heure et date de l'enregistrement et heure et date de la caméra »[69].

313. L'arrêté du 3 Août 2007 ne définit aucune contrainte d'interopérabilité, et les caractéristiques qu'il définit sont très en retard par rapport à la réalité technologique et aux besoins du terrain. C'est l'une des raisons pour lesquelles des travaux sont en cours pour sa mise à jour, mais ces travaux ne portent pas, à ma connaissance, sur la nécessité de formats communs.

314. ONVIF et PSIA sont deux initiatives industrielles[70] concurrentes pour définir un standard de communication entre équipements de vidéosurveillance et contrôle d'accès. Elles sont nées aux Etats 314. Unis, la première portée par le trio AXIS, Sony et Bosch, la seconde à l'initiative de Cisco. Leurs travaux sont intéressants, et de nombreux acteurs industriels se rallient à l'une ou l'autre, voir aux deux, de ces organisations, et les spécifications produites sont en permanente évolution. Le constat aujourd'hui est qu'elles permettent d'assurer une compatibilité minimum entre les fonctionnalités de bas niveau des équipements certifiés, mais ne garantissent en aucun cas l'interopérabilité envisagée.

315. Un groupe de travail (TC 79) a été constitué à l'IEC pour produire les normes IEC 62676-1 et 62676-2. Ces normes ont pour but de définir les caractéristiques techniques des équipements et les conditions de leur interopérabilité. Elles sont supposées faire converger les standards ONVIF et PSIA, mais les travaux n'ont fait que commencer, et les publications ne sont pas prévues avant fin 2014, voire au-delà.

5.3.4 Les critères minimum pour déclarer une technologie interopérable

316. Il reste encore un grand pas à franchir avant de parvenir à une liberté totale de choix entre les constituants d'un système global de sécurité électronique, et les donneurs d'ordre doivent en être informés en permanence. Les décisions d'investissement doivent tenir compte des évolutions potentielles de configurations, et les industriels qui se sont engagés dans une démarche d'ouverture doivent être privilégiés, pour éviter à terme la remise en cause d'un investissement initial conduisant à une impasse technologique potentielle.

317. En attendant la disponibilité d'une réelle interopérabilité, le Forum Open-IPVideo s'attache à étendre la notion de compatibilité, en définissant des critères minimum permettant de déclarer une technologie comme interopérable avec une autre[71].

[69] « L'évaluation d'algorithmes d'analyse vidéo – Quelques pistes », Jean-François Goudou, Louise Naud, Laurent Giulieri, Jaonary Rabarisoa, Olivier Pietquin, Dana Codreanu, Dijana Petrovska, Agence nationale de recherche (ANR), 7ème édition Workshop Interdisciplinaire sur la Sécurité Globale (WISG) 2013, http://www.agence-nationale-recherche.fr/Colloques/WISG2013/presentations/AAP10-Methodeo.pdf

[70] Onvif (Open Network Video Interface Forum) http://www.onvif.org/ et PSIA (Physical Security Interoperability Alliance) http://www.psialliance.org/ sont deux initiatives industrielles concurrentes pour définir un standard de communication entre équipements de vidéosurveillance et contrôle d'accès.

[71] Guide d'interopérabilité - Version 4 - avril 2014, Forum Open-IPVideo, info@open-ipvideo.org © Garry Goldenberg-Korn.

318. Pour être considérée comme interopérable, une technologie devra pouvoir fonctionner avec un minimum de trois solutions hétérogènes, offrant ainsi à l'utilisateur une liberté de choix et la sécurisation de ses investissements lors d'extensions ultérieures.

319. A titre d'exemple, selon le Forum Open-IPVideo :

- Une caméra doit pouvoir être gérée par trois modèles différents d'enregistreurs de marques différentes
- Un enregistreur doit être capable de gérer au minimum trois caméras de marques différentes
- Etc.

320. Par ailleurs, les équipements concernés devront satisfaire aux exigences règlementaires et normatives en vigueur sur les sites de déploiement, en l'occurrence :

- l'arrêté du 3 août 2007
- les normes EN 50132-7[72] et EN 50132-1:2010[73].

321.La norme européenne (norme EN 50132-7) donne des recommandations et des exigences pour choisir, planifier, installer, mettre en service, entretenir et essayer des systèmes de vidéosurveillance comprenant un(des) dispositif(s) de capture d'images, d'interconnexion et de traitement d'images, destiné(s) à être utilisé(s) dans des applications de sécurité.

5.3.5 La certification des installateurs

322.La problématique en termes de certification est réelle et nécessite de rappeler certaines notions car bon nombre de donneurs d'ordres et de professionnels ne font pas toujours la distinction entre l'agrément, le label, la qualification et la certification.

- L'agrément, le label est une simple formalité administrative. C'est la reconnaissance émise par une autorité qu'une personne ou une entreprise est apte à rendre un service donné dans des conditions bien précises. Dès lors, il s'agit surtout de demander à l'entreprise des pièces justificatives permettant d'assurer un minimum de sécurité et de sérieux au client et surtout d'avoir un pouvoir de contrôle sur ces entreprises dans le cas où des clients signaleraient des non-conformités. Le contrôle se fait plutôt a posteriori par la sanction possible du retrait de l'agrément par exemple.

- La qualification : Un certificat de qualification professionnelle est un certificat reconnaissant la compétence d'une entreprise par un organisme de qualification indépendant. Pour délivrer les certificats un organisme de qualification doit s'appuyer sur la norme NF X50-091.

- La certification : La certification est aujourd'hui un système juridique qui fait l'objet de définitions normatives et de contrôles. Dans ce cadre, l'un des instruments de la définition et du contrôle des entreprises certificatrices est le COFRAC à travers un arrêté permettant à toutes les sociétés certificatrices, sous réserve de respecter la réglementation, de pouvoir délivrer des certificats.

323. La certification est le dispositif le plus exigeant car la vérification des exigences est opérée par un organisme tierce partie, lui-même contrôlé en France par le COFRAC.

324.A ce jour il n'existe pas de certification de produits autre que les exigences règlementaires CE. Il s'agit donc d'une certification de services attribuée à une entreprise prestataire. Cette certification est volontaire et demandée par l'entreprise qui exerce ce domaine d'activité.

[72] Norme NF EN 50132-7 - Décembre 2012 - Systèmes d'alarme Surveillance CCTV usage applications sécurité - Partie 7: Lignes directrices.
[73] Norme EN 50132-1:2010 - Systèmes d'alarme – Systèmes de surveillance CCTV à usage dans les applications de sécurité – Partie 1: Exigences système.

325.Les dispositifs autres que la certification (agrément, label et qualification) n'ont pas de reconnaissance réelle pour la mise en œuvre de systèmes de videoprotection ou videosurveillance.

326. Les conditions de certification des installateurs de systèmes de vidéosurveillance sont fixées par L'arrêté du 5 janvier 2011[74].

327.Ce texte comporte une annexe qui définit le référentiel composé des exigences minimales à respecter par un installateur de systèmes de vidéosurveillance ainsi que des procédures de vérification que devra suivre un organisme certificateur pour vérifier que ces exigences sont satisfaites et délivrer le cas échéant un certificat reconnu par les préfectures, conformément à l'alinéa 11 de l'article 1er du décret n° 96-926 modifié.

328.En application du décret n° 2008-1401 du 19 décembre 2008, notamment ses articles 1er à 6, l'accréditation est prononcée par le Comité français d'accréditation (COFRAC) ou par tout organisme signataire de l'accord européen multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation, selon la norme EN 45011 assortie de règles d'application garantissant le respect par l'organisme certificateur des éléments figurant dans l'arrêté.

329.L'arrêté définit les acteurs de la certification comme suit :

- Le maître d'ouvrage, l'entité qui est responsable de la mise en place d'un système de vidéoprotection (collectivité locale, supermarché, banque, etc.).

- L'installateur, l'entreprise qui installera le système, suite à un contrat avec le maître d'ouvrage. Dans la mesure où l'autorisation délivrée par les préfectures est une autorisation préalable, l'installateur n'est en général que pressenti (suite à un devis), voire n'est pas encore connu (cas d'un appel d'offres).

- Le maître d'ouvrage peut donc s'engager à prendre un installateur titulaire d'un certificat délivré par un organisme certificateur, afin de bénéficier de la procédure simplifiée d'autorisation en préfecture.

- L'organisme d'évaluation de la conformité, ou organisme de certification, l'entité qui vérifie selon la procédure ci-après que les exigences minimales définies sont remplies par les installateurs et leur délivre le cas échéant un certificat.

330.Parmi les conditions de certification figurent les exigences minimales à respecter par les installateurs, telles que :

- La connaissance et la compréhension des exigences réglementaires de l'administration sur la vidéoprotection définit par le Code de la sécurité intérieure ;
- La réalisation avant toute prestation d'un devis comportant un descriptif technique, permettant notamment au maître d'ouvrage de justifier par lui-même la conformité de l'installation envisagée à ces mêmes exigences techniques ;
- La compétence technique pour conseiller utilement le maître d'ouvrage dans la mise en place des caméras, notamment sur le floutage des zones privatives, les conditions d'éclairage la nuit, les niveaux de sécurisation adapté ou encore contraintes d'exploitation ;

331. L'arrêté prévoit qu'avant la délivrance d'une certification à un installateur, l'organisme certificateur doit :

[74] JO du 14 janvier 2011.

- Effectuer une visite préalable d'au moins une demi-journée chez l'installateur, pour vérifier le respect des exigences légales ;
- S'assurer, par questionnaire ou entretien, que les connaissances des personnels leur permettent de réaliser des installations conformes aux exigences légales.
- Visiter au moins une installation réalisée chez un client.

332. L'organisme certificateur doit avoir le choix des clients qu'il souhaite contrôler (dès lors qu'il contrôle des installations sur des lieux recevant du public et que la confidentialité du fichier client de l'installateur est préservée).

333. En cas d'installations manifestement défectueuses ou non conformes à la réglementation détectées suite à des plaintes ou lors des visites de sondage, l'organisme certificateur doit adresser une mise en demeure à l'installateur. Si cette mise en demeure n'est pas suivie d'effet, l'organisme peut suspendre ou retirer sa certification à un installateur. Il doit alors en avertir le ministère de l'intérieur[75].

334.La certification n'est pas obligatoire, mais elle est un gage de la qualité technique du dossier de demande d'autorisation qui sera déposé en préfecture en ce qui concerne les systèmes de vidéoprotection relevant du Code de la sécurité intérieure[76].

335.Il existe deux dispositifs de certification pour les installateurs de systèmes de vidéoprotection. Cette certification permet d'alléger le dossier de demande d'autorisation en préfecture.

336.Ces dispositifs sont régis par des règlements de certification :

- « NF service et APSAD », mis en place et visée par le règlement de certification NF367-I82, organisée conjointement par l'AFNOR certification et le CNPP certification[77].

- mis en place par Bureau Veritas Certification accrédité par le COFRAC* en partenariat avec les spécialistes des solutions technologiques en Sûreté, Vidéoprotection et Détection Incendie.

5.3.5.1La certification AFNOR-CNPP

337.La certification APSAD est délivrée conjointement avec la certification NF Service. Le système des certifications conjointes NF Service & APSAD basé sur le référentiel NF 367-I82 est applicable depuis le 1er janvier 2009.

338.Le champ d'application de cette certification concerne :

- La conception et la réalisation
- La vérification initiale de conformité
- La maintenance préventive et corrective
- La vérification périodique de conformité.

339.Les caractéristiques certifiées sont :

- Les relations commerciales,
- La conception de l'installation (analyse de risque),
- La réalisation de l'installation,

[75] La réglementation de la certification des installateurs est disponible à l'adresse : http://www.interieur.gouv.fr/Videoprotection/La-certification-des-installateurs
[76] Voir 2.3 du présent livre blanc.
[77] Les installateurs intéressés peuvent contacter soit AFNOR certification, 11 rue Francis de Pressensé, F-93571 La Plaine Saint Denis cédex (tel. 01.41.62.86.88), soit le CNPP au département CNPP Certification, Route de la Chapelle Réanville, CD 64-BP 2265. F-27950 Saint Marcel (tel.02.32.53.64.00).

- La réception et la vérification de conformité initiale de l'installation,
- La maintenance,
- Les vérifications périodiques,
- Les dispositions d'organisation et de satisfaction des clients,
- Le personnel,
- Les moyens matériels,
- Le suivi du client.

340.Les entreprises certifiées font l'objet de contrôles systématiques par une tierce partie indépendante :

- D'audits des établissements concernés
- De visites d'installation.[78]

5.3.5.2La certification Bureau Veritas-SVDI

341. La certification Bureau Veritas en vidéosurveillance a pour objectif d'apporter aux clients les garanties que les entreprises sont contrôlées par des organismes de certification indépendants. Ces organismes vérifient les engagements de services :

- Un accueil et une écoute personnalisés
- Un lien contractuel sans ambigüité avec le client
- La maitrise et la gestion des prestations
- La compétence du personnel, au service de ses clients
- La maitrise des moyens matériels
- Le suivi des prestations techniques et de leur mise en œuvre
- L'engagement d'un service après-vente

342. Ils vérifient également l'évaluation des compétences techniques conformément au cadre défini par l'arrêté du 3 aout 2007 :

- Les exigences fonctionnelles sont connues
- Les exigences techniques de conception sont maitrisées
- Les exigences d'installations sont maitrisées
- Le processus d'auto contrôle est maitrisé
- La maintenance des installations est proposée et organisée

343. Les étapes de la certification Bureau Veritas-SVDI sont :

- Le respect des pré-requis (avoir obtenu l'agrément SVDI en vidéosurveillance ou avoir été reçu aux tests de compétences de PRESSELEC) ;
- La constitution du dossier de recevabilité pour chaque établissement. ;
- La signature du contrat de certification pour une période de 4 ans ;
- L'audit initial sur le terrain : un auditeur réalise l'audit selon le référentiel et les options retenues ;
- Le certificat remis à l'établissement, après avis favorable du Comité ;
- L'audit de suivi, tous les 16 mois.

344.Si l'installateur est déjà certifié il lui suffit de compléter le Cerfa par son nom et son numéro de certification et de délivrer à son client une attestation préalable de conformité, il s'engage ainsi à réaliser une installation conforme aux normes techniques définies par l'arrêté du 3 août 2007.

[78] Voir le détail de la certification AFNOR-CNPP sur le site CNPP : http://www.cnpp.com/DATA/tournepage/documentations/certifier/videosurveillance/index.html#/2/zoomed

345.Si l'installateur n'est pas certifié, il doit compléter le questionnaire succinct annexé à la notice associée au Cerfa. Il lui est recommandé par ailleurs pour les dispositifs complexes d'établir un rapport plus complet et précis.

5.3.6 La sécurité des réseaux

346. L'ANSSI (Agence nationale de la sécurité des systèmes d'information) a publié en février 2013 des recommandations de sécurité pour la mise en œuvre de dispositifs de videoprotection. Elles portent sur l'ensemble des composants d'un dispositif de vidéoprotection : déploiement physique des capteurs, architecture du réseau support, configuration des équipements et du centre de supervision[79].

347. Ces recommandations constituent un ensemble de mesures et de principes d'architecture, dont la mise en œuvre vise à contrer les vulnérabilités potentielles ou du moins, à en limiter l'impact, du fait de l'utilisation de technologies hertziennes et en particulier du Wifi.

348. Ces technologies séduisent de plus en plus de collectivités qui y voient un moyen de diminuer considérablement les coûts d'installation des dispositifs de vidéoprotection.

349. Or, selon l'ANSSI, « début 2013, près de la moitié des réseaux WiFi n'utilisent aucun moyen de chiffrement ou utilisent un moyen de chiffrement obsolète ».

350. C'est la raison pour laquelle elle recommande de recourir à des systèmes cryptographiques pour protéger les données transmises, d'avoir un réseau dédié, non relié au SI et de cloisonner le réseau pour éviter qu'une caméra piratée ne se transforme en cheval de Troie donnant accès à l'ensemble du système.

351. L'ANSSI résume les risques liés à l'exploitation d'éventuelles vulnérabilités dans les dispositifs de vidéoprotection en trois catégories :

- Atteinte à la confidentialité des données de vidéoprotection : les flux vidéo et éventuellement audio captés par les caméras peuvent être interceptés, par écoute passive sur le réseau support ou interception de rayonnements parasites compromettants. La sensibilité des flux qui sont susceptibles d'être interceptés dépend naturellement du positionnement des caméras à l'intérieur ou à l'extérieur des locaux qu'elles contribuent à protéger.

- Atteinte à la disponibilité de la vidéoprotection : l'exploitation de vulnérabilités logiques dans les différents équipements actifs du réseau de vidéoprotection (caméras, équipements de routage, serveurs de collecte) peut permettre à un attaquant de désactiver tout ou partie du dispositif. Une attaque de ce type peut par ailleurs être dissimulée par l'injection de flux vidéo illégitimes créés par l'attaquant ou le rejeu de flux légitimes antérieurs.

- Intrusion dans le reste du système d'information : lorsque le réseau support des équipements de vidéoprotection est mutualisé avec le système d'information de l'entité utilisatrice (réseau bureautique, serveurs internes ou externes), la prise de contrôle d'un équipement de vidéoprotection par un attaquant peut permettre à ce dernier de mener dans un second temps une intrusion plus générale au sein du système d'information. Ce risque est d'autant plus significatif que, de par la nature même de leur fonction, les caméras de vidéoprotection sont souvent plus exposées à des attaques physiques que les autres équipements du système d'information (caméras déployées à l'extérieur des bâtiments, ou dans des zones peu fréquentées).

352. L'ANSSI préconise :

[79] Recom. N°524/ANSSI/SDE du 14-2-2013 pour la mise en œuvre de dispositifs de vidéoprotection, disponibles : http://www.ssi.gouv.fr/IMG/pdf/videoprotection_notetechnique_anssi.pdf

- Le cloisonnement et l'isolement de l'architecture du réseau support, par rapport au reste du système d'information ;
- Le recours au chiffrement et à l'authentification des flux réseau émis et reçus par les équipements ;
- La sécurité du centre de supervision, en termes de sécurité physique mais aussi et surtout sur l'application de règles strictes d'hygiène informatique ;
- La prise en compte de la problématique des signaux compromettants (rayonnements électromagnétiques parasites) selon les modalités définies par la réglementation en vigueur [80];
- En cas de recours à une externalisation du service, la nécessité de passer par le respect de bonnes pratiques organisationnelles et contractuelles, selon la démarche décrite dans le guide « Maîtriser les risques de l'infogérance – externalisation des systèmes d'information » publié par l'ANSSI[81].

5.4 Constats et propositions du groupe de travail

5.4.1 Sur la mobilité

353.En ce qui concerne la mobilité à l'aide de caméras embarquées, il y a actuellement un vide juridique quant aux autorisations à solliciter et aux textes réglementaires à respecter avant de mettre ce type d'outil à disposition des municipalités.

354. Les expérimentations actuellement en cours auprès des fonctionnaires de police et militaires de la gendarmerie nationales devraient aboutir prochainement à un projet d'arrêté-cadre annoncé par le ministre de l'intérieur.

355.Il semblerait que ce texte en cours de préparation soit limité à la police nationale et à la gendarmerie qui ont été l'objet des expérimentations. Néanmoins de nombreuses municipalités ont déjà doté leur police municipale de ce type d'équipement.

356.Il conviendrait que ce projet de texte soit généralisé à la police municipale, cette dernière ayant vu ses pouvoirs judiciaires (répression) se développer ces dernières années.

357. Son action est en effet complémentaire à celle de la police nationale et de la gendarmerie. La police municipale peut être amenée à interpeller l'auteur d'une infraction, dans le cadre d'un flagrant délit. Elle devrait donc également pouvoir recourir à des caméras embarquées.

5.4.2 Sur la mutualisation des images et l'interopérabilité des systèmes

358.En ce qui concerne la mutualisation des images, la législation actuelle ne permet pas de mutualiser les visualisations et reports d'images émanant à la fois de lieux publics et privés. Or, se raccorder à des réseaux privés peut, dans certains cas, garantir une réactivité accrue et adaptée des forces de l'ordre, par exemple.

359. Aussi, la mutualisation de centres de supervision urbains (CSU) ou PC sécurité ou bien des interconnexions à des sites sensibles comme des centres commerciaux, grands magasins, etc., pourrait permettre de convenir, conjointement, de l'échange de contenus, de flux en temps réel et/ou en temps différé, qu'il y ait réquisition ou non d'images.

360. L'image en temps réel et sans discontinuité est très importante, notamment dans le cadre de filature d'un suspect.

361. Il devrait être possible d'assouplir le dispositif sans remettre en cause les missions d'exploitation et de contrôle des images produites par les caméras de vidéoprotection qui doivent être assurées par l'autorité publique compétente et non par un partenaire privé.

[80] www.ssi.gouv.fr/fr/reglementation-ssi/signaux-parasites-compromettants-spc.
[81] www.ssi.gouv.fr/externalisation.

362. Il est en effet dommage de se priver d'images qui révèlent des délits. Une des pistes à explorer serait de tendre vers une plus grande mutualisation de l'exploitation des images selon des modalités juridiques et techniques à définir. Cela permettrait également de mutualiser les coûts des centres de supervision urbains entre les communes ou avec des organismes non municipaux (centres hospitaliers, SNCF, sociétés de transport)[82].

363. Ces dispositifs ont commencé à être mis en place sur Paris, notamment via des conventions de partenariat. Aujourd'hui, la Préfecture de Police peut accéder, en temps réel, au réseau de la RATP, de la SNCF, voire même à certains centres commerciaux et magasins mettant à disposition leurs systèmes de vidéoprotection (Printemps, Forum des Halles, Les Quatre Temps, Rosny 2, etc.), soit près de 20 000 caméras pour un maillage performant[83].

364. Aujourd'hui, la technologie facilite la mutualisation des capacités de stockage dans une infrastructure partagée, fiable, sécurisée et donc synonyme d'économies d'échelle.

365. Il conviendrait de trouver un compromis relatif à la mutualisation des images afin de favoriser les initiatives prises par certaines collectivités, aujourd'hui, pour créer un CSU dédié aux bailleurs sociaux.

Propositions du groupe de travail

- Créer un cadre juridique commune aux forces de l'ordre et à la police territoriale en ce qui concerne le port de caméras piétons
- Généraliser la signature de conventions de partenariat entre le secteur public et privé pour développer la mutualisation des images
- Confier l'interopérabilité à un organisme dédié pour favoriser la généralisation de la mutualisation

[82] Voir le rapport d'information sur la contribution de l'État au développement de la vidéoprotection présenté à l'Assemblée nationale le 13 juillet 2010, Rapport AN 2728, http://www.assemblee-nationale.fr/13/pdf/rap-info/i2728.pdf

[83] Voir http://www.aasset-security.com/newsletter/2014/01_aasset_paris/index.html

6. Sous-groupe : Le statut des vidéo opérateurs

366. La vidéo-protection est un outil efficace de lutte contre les nouvelles formes d'insécurités urbaines. Elle ne se substitue en aucun cas aux actions de prévention et de sécurité menées par les forces de l'ordre (PM-PN), mais représente un complément efficace aux dispositifs existants. A travers ce nouvel équipement, les municipalités se sont fixées pour objectif de lutter activement contre les incivilités.

367.La vidéo-protection peut prévenir la délinquance dans certains lieux, tout comme elle peut la déplacer. Avant tout, elle reste une arme supplémentaire pour les forces de l'ordre et elle permet de faciliter l'élucidation rapide, des crimes et des délits.

368. Elle permet également de mieux déterminer les responsabilités lors d'accidents routiers, d'améliorer l'entretien des espaces verts, de signaler tout dysfonctionnement de la voie publique aux services techniques des collectivités et de venir plus rapidement en aide aux victimes.

369.L'action des forces de l'ordre (PN/PM), appuyée par cet outil, produit des résultats tangibles. Elle permet d'effectuer de nombreuses interpellations en flagrant délit et surtout d'anticiper des situations explosives entre bandes rivales dans certaines villes exposées à ces phénomènes de délinquance.

6.1 Définition des fonctions des vidéo opérateurs

370. La vidéo protection constitue un véritable métier. L'opérateur doit réunir des compétences avérées. Il doit pouvoir détecter des comportements suspects, des rassemblements potentiellement dangereux, connaître parfaitement les lieux vidéo-surveillés et leurs possibilités de fuite ou de cachette, afin d'anticiper le comportement des délinquants. En d'autres termes, il doit avoir «le flair policier» ou le «goût de la chasse», et savoir réagir rapidement aux diverses infractions repérées sur les écrans.

6.1.1 Les activités de vidéo opérateur

371. L'Opérateur de vidéo surveillance ou protection assure la sécurisation préventive et curative des lieux, des espaces et des bâtiments dotés d'équipements de vidéosurveillance. Il visionne et exploite les informations en vue d'informer les partenaires chargés d'intervenir sur les sites.

372. Ses activités principales sont de :

- Repérer sur écran des événements significatifs ;
- Rechercher des informations à partir d'images enregistrées ;
- Gérer la traçabilité et l'archivage des images ;
- Gérer la destruction des images en fonction de la réglementation et des procédures en vigueur ;
- Déclencher des outils ou des actions correspondant aux différents types d'alarme ;
- Collecter et analyser les informations issues des observatoires ;
- Participer aux coordinations chargées des plans de surveillance et d'intervention ;
- Programmer et vérifier les masques et champs de vision ;
- Signaler les pannes auprès des interlocuteurs compétents ;
- Alerter les responsables hiérarchiques sur les dysfonctionnements des procédures ;
- Formuler des propositions d'optimisation des modes opératoires, des procédures et de l'exploitation du cycle des images ;
- Assurer la prise en compte et la transmission des consignes entre agents et auprès des responsables ;
- Organiser les moyens techniques et humains pour assurer la continuité du service de vidéosurveillance.

6.1.2 Les catégories de vidéo opérateurs

373. Il existe plusieurs catégories de vidéo opérateurs :

- Vidéo opérateur travaillant dans un CSU en charge de surveiller la voie publique : cette personne est salariée de la commune la communauté de communes l'agglomération. Elle ne dispose pas de carte professionnelle délivrée par le Cnaps (Conseil national des activités privées de sécurité) ;

- Vidéo opérateur travaillant dans un lieu ouvert au public, par exemple une grande surface. Cette personne a pour mission la sécurité de l'établissement ainsi que la lutte contre la démarque inconnue. Elle peut être salariée de l'établissement (service interne de sécurité ou d'une entreprise de sécurité privée) dans les deux cas elle doit être titulaire d'une carte professionnelle délivrée par le Cnaps ;
  -
- Vidéo opérateur de télévideosurveillance en charge d'assurer des rondes vidéo à distance dans des lieux privés secteur tertiaire ou industriel et commercial. Cette personne doit être titulaire d'une carte professionnelle délivrée par le Cnaps ;

- Opérateur en station de télésurveillance utilisant des images pour lever le doute d'une alarme reçue : Attention le dispositif installé sur le site sécurisé n'entre pas dans le champ des systèmes soumis à autorisation préfectorale. Il s'agit la plupart du temps de capteur image faible résolution sans véritable flux vidéo ne permettant pas l'identification mais simplement de comparer une image de référence attestant d'une présence humaine sur un site censé être inoccupé. Cette personne doit être titulaire d'une carte professionnelle délivrée par le Cnaps

374. Par ailleurs, il existe une formation OSTID développée par le Gpmse que l'opérateur pourra suivre afin d'obtenir l'examen attestant de son niveau de qualification pour l'obtention de sa carte professionnelle.

6.2 Le statut de la profession

Selon la nature du dispositif, il y a deux cas de figures :
- Fonction publique
- Hors fonction publique

6.2.1 Secteur public

375. Les personnes pouvant accéder aux enregistrements visuels de vidéoprotection sur la voie publique sont :

- Les personnes habilitées qui ont été mentionnées sur l'autorisation préfectorale (rubrique 6 du formulaire CERFA) ;
- Uniquement dans le cadre de leur fonction.

376. Actuellement, cette habilitation ne dépend pas d'une qualification ou d'une formation diplômante mais du seul statut d'agent de la fonction publique.

377. L'opérateur(trice) est en effet soumis(e) aux conditions d'accès des agents de la fonction publique.

378.Actuellement, les capacités attestées et le descriptif des composantes de la certification sont :

1. Assurer la surveillance visuelle d'un lieu à l'aide de moyens de vidéosurveillance ou de vidéoprotection :

- Contrôler les accès par un système de vidéosurveillance ou de vidéoprotection.

- Analyser et exploiter les images provenant d'un système de vidéosurveillance ou de vidéoprotection pour sécuriser des sites.
- Veiller au fonctionnement du système vidéo en centre d'exploitation.

2. Gérer la sécurité des personnes et des biens et réguler l'organisation des interventions au moyen d'un dispositif de télésurveillanc :

- Traiter les informations et s'assurer du retour de fonctionnement à la normalité des systèmes de sécurité.
- Déclencher l'intervention des personnes habilitées en cas d'alarme ou d'anomalie et des services compétents en cas de levée de doute positive.
- Réguler l'organisation des interventions.
- Veiller au fonctionnement et à la sécurité de la station centrale de télésurveillance.
- Réceptionner et assurer le traitement des communications.

379.Dans le secteur public, la Préfecture de Police a mis en place une formation des utilisateurs du PVPP.

380.Les règles d'usage du PVPP précisent que l'accès à ce système est nécessairement conditionné par une formation préalable. Aussi, toutes personnes qui souhaitent accéder aux images du PVPP doit avoir été, préalablement, formées à utiliser le système et sensibiliser aux enjeux de la vidéoprotection.

381.Les utilisateurs suivent une formation se déroulant entre 2 et 4 jours en fonction de leur rôle et de leur degré de responsabilité sur le système. La formation aborde l'ensemble des règles régissant la vidéo-protection et notamment, l'éthique. Concernant les points techniques, la formation dispensée est marquée par les particularités du système PVPP et de ses utilisateurs à savoir les forces de police.

382.À ce jour, un peu plus de 3500 fonctionnaires (essentiellement des fonctionnaires de police) ont été formés à utiliser le PVPP. Les demandes de formation sont croissantes et confirment l'intérêt des forces de police pour cet outil de vidéoprotection.

6.2.2 Secteur privé

383. La vidéoprotection fait partie du champ des activités privées réglementées de sécurité[84]. Depuis mars 2012, la loi n°83-629 régissant la sécurité privée a été intégrée dans le Code de la sécurité intérieure (CSI).

384. Son article L613-13 prévoit que les opérateurs privés de vidéosurveillance visionnant la voie publique ou des lieux ouverts au public sont soumis au CSI. A ce titre, tout opérateur chargé de visionner des images, qu'il appartienne à une société privée prestataire de services ou à un service interne, doit être détenteur d'un numéro de carte professionnelle susceptible de lui être délivré au regard de ses antécédents et de la possession d'une attestation de formation en lien avec son activité.

385. Cette disposition peut donc concerner tout agent travaillant dans un parking, un magasin, un PC autoroutier.

386. Dans un communiqué du 11 septembre 2012[85], Alain Bauer, a précisé qu'actuellement, « toute formation, titre ou certification de qualification professionnelle (CQP) concernant le champ de la surveillance par des moyens humains ou électroniques permet d'obtenir la carte professionnelle d'opérateur de vidéoprotection ».

[84] Décret n° 2011-1919 du 22 décembre 2011.
[85] A. BAUER, Président du CNAPS, Communiqué du 11-9-2012.

387. Les décrets et arrêtés[86] réglementant les activités privées de sécurité et l'aptitude professionnelle des dirigeants et des salariés exerçant une activité de vidéoprotection prévoient la formation du vidéo opérateur sans toutefois en définir expressément le contenu.

388. Les activités privées de sécurité nécessitent la délivrance d'une carte professionnelle d'agent privé de sécurité ou l'obtention d'une autorisation préalable en application du Livre VI du Code de la sécurité intérieure.

389. Les formalités s'exercent auprès du Conseil national des activités privées de sécurité (CNAPS)[87].

390. L 'opérateur(trice) en surveillance à distance assure la sécurité des sites des clients professionnels et des particuliers en traitant les alarmes et/ou les images provenant des systèmes de vidéosurveillance ou de vidéoprotection dans le respect de la réglementation qui s'applique à ce métier.

391. En vidéosurveillance ou en vidéoprotection, l'opérateur(trice) analyse et exploite les images provenant des écrans pour assurer une veille continue sur les lieux, espaces ou bâtiments qu'il (elle) doit surveiller.

392.Les activités de vidéosurveillance ou de vidéoprotection et de télésurveillance sont exercées indépendamment ou de façon complémentaire, seul(e) ou en équipe sous la responsabilité d'un supérieur hiérarchique. Néanmoins, l'opérateur(trice) doit être autonome dans ses actions et responsable de ses choix dans le respect des procédures et des consignes. Il (elle) respecte la confidentialité des informations et rend compte à sa hiérarchie.

393. Dans le cadre de la continuité de service, il (elle) est en contact permanent avec les autres salariés et avec les clients, les intervenants et les services de secours. La gestion simultanée d'informations et de tâches est pratique courante.

394. La connaissance des fondamentaux de la protection et de l'alerte est requise.

395. La pratique de formules courantes dans une langue étrangère peut être demandée.
Il (elle) peut exercer d'autres activités liées à la surveillance à distance telles que la géolocalisation des personnes et des véhicules.

396. L'emploi de l'opérateur(trice) est sédentaire et s'exerce en position assise dans un centre d'exploitation constitué d'écrans de réception d'informations. En vidéosurveillance ou en vidéoprotection, l'amplitude horaire varie en fonction de l'activité. En télésurveillance, l'opérateur(trice) peut travailler de jour comme de nuit, week-ends et jours fériés. Il (elle) peut exercer dans des contextes spécifiques tels que la téléassistance ou le téléservice. L'accès à la profession est réglementé et nécessite une carte professionnelle[88].

397. La certification de qualification professionnelle d'agent de prévention et sécurité (CQP APS) a été modifié en juillet 2012[89]. Le « CQP APS 2 » intègre désormais un module technique intitulé, « Télésurveillance et vidéoprotection », d'une durée minimale de 8 heures, dont 5 heures de mise en situation pratique.

398. Les objectifs pédagogiques généraux de ce module sont les « Systèmes de télésurveillance et de vidéosurveillance ».

399. Les objectifs pédagogiques spécifiques sont de maîtriser :

- — le corpus juridique de la télésurveillance et de la vidéosurveillance ;
- — la chaîne de télésécurité ;

[86] Décret 2005-1122 du 6 septembre 2005 et arrêtés d'application du 18 janvier 2013 et du 1er juin 2013.
[87] Voir : http://www.cnaps-securite.fr/vos-demarches/carte-professionnelle/
[88] Sur les missions et activités, voir http://infos.emploipublic.fr/metiers/liste-des-metiers/securite-prevention/operateur-de-video-surveillance/apm-2846/
[89] Arrêté du 10 juillet 2012 modifiant l'arrêté du 3 août 2007 : JO du 22 juillet 2012.

- — le schéma d'installation de la vidéosurveillance.

400. Le « CQP APS 2 » est agréé pour une durée de trois ans à compter du 1er janvier 2013[90].

6.3La formation d'opérateur de vidéoprotection ou Opérateur en télésurveillance ou Télévidéosurveilleur

401. Le titre d'« Opérateur vidéo protection » (ou Opérateur en télésurveillance ou Télévidéosurveilleur) est référencé dans le Répertoire National des Certifications Professionnelles (RNCP) sous le Code NSF.

402. La certification de qualification professionnelle d'agent de prévention et sécurité (CQP APS) a été modifiée en juillet 2012[91]. Le « CQP APS 2 » intègre désormais un module technique intitulé, « Télésurveillance et vidéoprotection », d'une durée minimale de 8 heures, dont 5 heures de mise en situation pratique.

403. Les objectifs pédagogiques généraux de ce module sont les « Systèmes de télésurveillance et de vidéosurveillance ».

404. Les objectifs pédagogiques spécifiques sont de maîtriser :

- — le corpus juridique de la télésurveillance et de la vidéosurveillance ;
- — la chaîne de télésécurité ;
- — le schéma d'installation de la vidéosurveillance.

405. Le « CQP APS 2 » est agréé pour une durée de trois ans à compter du 1er janvier 2013[92].

6.3.1 Le titre d'Opérateur vidéo protection ou Opérateur en télésurveillance ou Télévidéosurveilleur

406. Le résumé descriptif de la certification d'opérateur vidéo protection figurant au Répertoire National des Certifications Professionnelles (RNCP) est le suivant :

— « 344 Sécurité des biens et des personnes, police, surveillance »[93].

407. Selon le résumé du référentiel d'emploi ou éléments de compétence acquis, le titulaire de la certification d'« Opérateur vidéo protection » réalise les activités suivantes :

— Prise en compte d'un Centre de Supervision Urbain (CSU).
- Assurer la sécurité d'un CSU.
- Exploiter un système de vidéo protection urbain
- Gérer un système de traitement des alarmes des sites raccordés (Télésurveillance).
- Déclencher et assurer le suivi des interventions selon la typologie des évènements.
- Assurer les aspects techniques et la communication de la gestion des crises ou des grands évènements.
- Rendre compte.

— Compétences et capacités techniques:
- connaissance des matériels et des technologies

[90] Arrêté du 28 août 2012 : JO du 6 septembre 2012.
[91] Arrêté du 10 juillet 2012 modifiant l'arrêté du 3 août 2007 : JO du 22 juillet 2012.
[92] Arrêté du 28 août 2012 : JO du 6 septembre 2012.
[93] Voir : http://www.rncp.cncp.gouv.fr/grand-public/visualisationFiche?format=fr&fiche=14581 en annexe du présent livre blanc.

- application des procédures
- connaissance du cadre légal et règlementaire
- Maîtrise des situations d'alerte

— Compétences et capacités comportementales:
- Transmissions; application des consignes
- Capacités de communication
- capacité de concentration, gestion du stress
- travail en équipe mais aussi en autonomie
- Discrétion, respect de la confidentialité et des règles déontologiques

408. L'opérateur vidéo protection est capable :
— d'appliquer strictement des procédures techniques, transmettre clairement des consignes ;
— de maîtriser une situation d'alerte ;
— de communiquer clairement ;
— d'une attention soutenue pendant un temps relativement long ;
— de faire preuve de discrétion.

409. Avec ce titre ou ce certificat, l'opérateur exerce ses fonctions dans :
— les villes ou communautés d'agglomération ;
— les PC de sûreté dans les transports publics ;
— les salles de vidéo surveillances dans les entreprises recevant du public ou les grands sites industriels.

410. Le descriptif des composantes permettant d'accéder à la certification :

1) QCM contrôle écrit des connaissances en matière de :
- Législation, réglementation, déontologie, normes
- Procédures
- Statistiques et caractéristiques de la délinquance
- Techniques et technologies
- Différents services intervenants et leurs prérogatives

2) Entretien évaluation :
- La maîtrise de la langue française
- Capacités de transmission des informations
- De demande des consignes
- Relation d'un événement, d'une situation
- Signalement d'une personne, d'un véhicule, d'une scène

3) Mise en situation :
Epreuve d'analyse d'une scène filmée, avec exercice de transmission de l'alerte (téléphone, radio) et relation écrite.

6.3.2 Les formations du CNFPT

411. Le CNFPT (Centre national de la fonction publique territoriale) dispense une formation d'opérateur de vidéoprotection (Fiche 04/E/34)[94] fonction exercée en centre de vidéoprotection[95].

412.Cette formation contribue à la sécurisation des lieux, des espaces et des bâtiments publics au moyen d'une vidéoprotection en exploitant les images en vue d'informer les partenaires chargés d'intervenir sur les sites.

[94] Voir http://www.cnfpt.fr/ws/rmt/pdf/fiche/?id_metier=135&gl=NjliOGJkMzI en annexe du présent livre blanc.
[95] Code Rome E/M K2503 « Sécurité et surveillance privées ».

413.L'objectif de cette formation est d'identifier les bases réglementaires et les outils de communication pour assurer les fonctions d'opérateur de vidéo-protection.

414.Le contenu de cette formation qui dure 5 jours est le suivant :

- -Définition des prérogatives de l'opérateur de vidéo-protection à travers son cadre légal.
- -Notions élémentaires de droit pénal.
- -Notions de la réglementation sur l'exploitation des images.
- -Responsabilités administratives et pénales.
- -Comportements et postures professionnelles.
- -Procédures et règles de confidentialité.
- -La gestion des alertes opérationnelles.
- -La transmission des informations à ses partenaires

415.L'accès à cette formation se fait par concours externe et interne avec conditions de diplôme et/ou examen d'intégration en fonction du cadre d'emplois, concours troisième voie. Il y a également une possibilité de recrutement direct pour les cadres d'emplois de catégorie C en fonction du grade (deuxième classe).

6.3.3 Les formations du CNPP

416. Le CNPP (Centre national de prévention et de protection) dispense deux formations[96] :

- opérateur privé en vidéosurveillance (VIDEOPRIV)
- opérateur public en vidéosurveillance (VIDEOPUB)

417. Chacune de ces formations dure 5 jours et a pour objectifs :

- Pour les opérateurs en station de vidéosurveillance privée (entreprise, grande distribution, etc.) titulaires d'une carte d'agent de prévention et de sécurité :
    - Exercer une activité de vidéosurveillance privée en conformité avec le cadre juridique et réglementaire ainsi que la déontologie propre à la profession.
    - Assurer la sécurisation préventive et curative de lieux privés dotés d'équipements de vidéosurveillance.
    - Visionner et exploiter les informations en vue d'informer les partenaires chargés d'intervenir sur les sites.

- Pour les opérateurs en vidéoprotection affectés en Centre de Supervision Urbain, issus des filières : police municipale, administrative ou technique de la fonction publique territoriale :
    - Assurer la sécurisation préventive et curative des lieux, des espaces et des bâtiments publics dotés d'équipements de vidéosurveillance.
    - Visionner et exploiter les informations en vue d'informer les partenaires chargés d'intervenir sur les sites

418. La formation d'opérateur privé s'adresse à des APS (agents de prévention et de sécurité) déjà agréés désirant augmenter leurs compétences.

419. Elle est structurée autour de 4 modules :
- MODULE 1 - Cadre juridique et déontologique - 2 jours
- MODULE 2 - Technologie - 1 jour
- MODULE 3 - Méthodologie professionnelle - 1 jour

[96] Voir le catalogue de formation en ligne sur le site http://www.cnpp.com/fr/ et annexe du présent livre blanc.

- **MODULE 4 - Application - 1 jour**

420. La formation d'opérateur public est structurée autour de 3 modules :
- MODULE 1 - Cadre juridique - 3 jours
- MODULE 2 - Méthodes de surveillance et procédures d'exploitation - 1 jour
- **MODULE 3 - Application - 1 jour**

6.3.4 Les formations des GRETA

421. Les Greta (organismes de formation continue de l'Education Nationale) organisent des formations pour adultes dans les métiers de la sécurité, notamment le GRETA 34 Ouest (Lycée Jean Moulin, Languedoc-Roussillon – Hérault, 34 BEZIERS)[97].

422.Le contenu de cette formation qui dure 70 h est le suivant :

- Cadre légal et réglementaire de la vidéo protection
- Aspects déontologiques et comportementaux
- Environnement quotidien de l'opérateur
- Utilisation de l'outil
- Gestion de crise

423. Cette formation n'est pas réservée aux employés de collectivités territoriales. Elle s'adresse à tous adultes demandeurs d'emploi et salariés d'entreprises de sécurité.

6.3.5 Les formations diplômantes AFPA

424. L'Association nationale pour la Formation Professionnelle des Adultes (AFPA) propose des formations certifiées de niveau IV d'une durée modulable de 4 mois (525 heures) à 10 mois environ (1400 h.) :

- Opérateur en surveillance à distance98 comportant un socle de base des aptitudes professionnelles en sécurité privée (connaissances réglementaires 2 semaines).;
- — Technicien en systèmes de surveillance - intrusion et de videoprotection (ex-TISI)[99]

425. Certaines de ces formations sont également proposées en alternance et en validation des acquis et de l'expérience (VAE)[100].

6.3.6 La formation d'opérateur en station de télésurveillance GPMSE

426. Le Groupement des métiers de la sécurité électronique (GPMSE) travaille depuis plusieurs années sur les problématiques de formation à la télésurveillance.

427.Il propose une formation d'opérateur en station de télésurveillance (OSTISD).

428.Le titre OSTISD déposé au RNCP, Opérateur(trice) spécialisé(e) en traitement d'informations à distance, porté par le GPMSE Télésurveillance concerne la formation de l'opérateur en station de télésurveillance et permet l'accès aux métiers Opérateur en Télésurveillance et Opérateur en Télévidéosurveillance. Pour l'opérateur en Télévidéosurveillance on doit distinguer 2 catégories : l'opérateur en charge de la surveillance d'un site industriel la nuit en l'absence de personnel, il s'agit là de la lutte contre la malveillance et les

[97]Voir http://greta34ouest.fr/secteur-securite/operateur-de-video-protection.html en annexe du présent livre blanc.
[98] Code Rome: K2503 ; Formacode : 42801 ; Code AFPA : 11514 ; Fiche formation disponible sur : http://www.afpa.fr/formations/les-offres-de-formation-et-vae/formation-diplomante/fiche/11514
[99] Code Rome: F1602-I1305 ; Formacode : 42801 ; Code AFPA : 5228 ; Fiche formation disponible sur : http://www.afpa.fr/formations/les-offres-de-formation-et-vae/formation-diplomante/fiche/5228
[100] La carte professionnelle ou l'autorisation préalable sont exigées dans le cadre de la VAE.

cambriolages et par ailleurs l'opérateur exerçant une mission de lutte contre la démarque inconnue par exemple la surveillance de clients dans un hypermarché ou une grande surface de bricolage

429.Il apparaît nécessaire à terme, que des modules complémentaires soient créés au fur et à mesure de l'arrivée de nouvelles technologies (ex opérateur vidéo exerçant à partir d'un drone) .

430.L'avantage de passer par la formation initiale OSTISD permet des passerelles entre les différents métiers et rend plus attractif l'intérêt porté à ces nouveaux métiers.

431.L'opérateur en télésurveillance est un agent de sécurité qui travaille dans une station centrale de réception des alarmes. Il doit s'assurer de la réception et du traitement des informations reçues et de l'application des consignes définies. Il travaille dans un service de télésurveillance et/ou de permanence opérationnelle assurant la réception des alarmes. Ses missions consistent principalement à traiter les informations reçues, à déclencher l'intervention des personnes habilitées et appeler les services compétents, à effectuer le suivi des rondiers intervenant au cours de leurs missions et à s'assurer du retour à la normalité de fonctionnement (Source : Syndicat national des entreprises de sécurité, http://www.e-snes.org/emploi.html).

432. Le titre professionnel d'opérateur(trice) spécialisé en traitement d'informations de sécurité à distance (OSTISD) correspond à un titre professionnel de « niveau IV », c'est-à-dire équivalent à celui du Brevet Professionnel (BP), du Brevet Technicien (BT), du Baccalauréat Professionnel ou du Baccalauréat Technologique.

433.Le titre OSTISD proposé par le GPMSE correspond à un Certificat de Qualification Professionnelle (CQP) enregistrée au répertoire national des certifications professionnelles, se rapportant à l'activité d'opérateur de station de télésurveillance.

434.La formation est dispensée aux personnels exerçant leur activité dans les stations centrales de télésurveillance, centres de contrôle et de traitement d'informations à distance, centres de sécurité et de supervision.

435.A l'issue d'une formation de 156 heures (dont 41 Heures consacrées à la réglementaire et à la déontologie et 115 Heures consacrées au métier), les stagiaires passent un examen de 2 heures (Questions écrites sous forme de QCM, entretien devant un Jury et mise en situation).

436. La formation d'opérateur en station de télésurveillance proposée par le GPMSE contient un module concernant l'environnement règlementaire :

– Environnement juridique de la sécurité privée consistant à :
- Etude Livre VI du Code de la Sécurité intérieure
- Maîtriser :
    - – l'explication initiale du livre VI (contexte, logique) ;
    - – l'architecture d'ensemble ;
    - – les conditions d'accès à la profession (moralité et aptitude professionnelle) ;
    - – le principe d'exercice exclusif ;
    - – le principe de neutralité ;
    - – la détention et usage des armes ;
    - – le port des uniformes et insignes ;
    - – les dispositions visant à éviter la confusion avec un service public et sanctions (avec cas concrets) ;
    - – les spécificités des services internes ;

- – le régime de la carte professionnelle DRACAR et téléc@rtepro[101]. Le cnaps son rôle et exigences.

– Connaître les dispositions utiles du code pénal, à savoir :
- Maîtriser les concepts de légitime défense, de faits justificatifs comme l'état de nécessité, d'atteinte à l'intégrité physique et à la liberté d'aller et venir :
  - – les conditions légales de rétention d'une personne avant mise à disposition des forces de police ;
  - – la non-assistance à personne en danger ;
  - – l'omission d'empêcher un crime ou un délit ;
  - – l'usurpation de fonctions ;
  - – l'atteinte aux systèmes de traitement automatisé ;
  - – l'appropriation frauduleuse ;
  - – le fonctionnement des juridictions pénales.

– Application de l'article 73 du code de procédure pénale :
- Savoir respecter les conditions d'interpellation de l'article 73 du CPP ;
- Maîtriser les garanties liées au respect des libertés publiques.

– Connaître la législation relative :
- au respect de la vie privée ;
- au respect du droit de propriété ;
- aux juridictions civiles ;
- à la CNIL.

– Respecter la déontologie professionnelle :
- Respecter :
  - le secret professionnel ;
  - les principes déontologiques. Etre averti sur les marchandages et les sanctions spécifiques associées.

6.3.7 Les autres initiatives

437. La liste des formations au métier d'opérateur de vidéoprotection n'est pas exhaustive ; il existe de nombreux autres organismes qui proposent des formations qui peuvent répondre aux attentes de la profession dès lors qu'elles contiennent un minimum requis qui reste toutefois encore à fixer.

438. Il convient également de signaler l'initiative la CAVAM (Communauté d'agglomérations de la vallée de Montmorency) précusseur en matière de vidéoprotection.

439. Elle a mis en service le premier système de vidéoprotection intercommunal de France, en février 2007[102], situé dans l'enceinte du Commissariat Subdivisionnaire de Police Nationale de Montmorency et a implanté un Centre de Supervision Urbain (CSU) de formation sur la commune de Soisy-sous-Montmorency, pour permettre à des organismes de formation de venir se former.

440. En partenariat avec le CNFPT, les salles du CSU de formation sont mises à la disposition de stagiaires (opérateurs en poste ou en devenir auprès de communauté d'agglomération et/ou de mairie) qui bénéficient ainsi de formations in situ dispensées par des formateurs agréés par le CNFPT.

441. La CAVAM a eu pour préoccupation, dès le départ, de dispenser à l'ensemble de ses opérateurs une formation adaptée en partenariat avec le CNFPT[103].

[101] Voir https://telecartepro.interieur.gouv.fr/telecartepro.htm
[102] Voir : http://www.valdoise.fr/9808-la-video-protection-de-la-cavam-presentee-par-son-president.htm
[103] Voir http://www.interieur.gouv.fr/Videoprotection/Documentation/La-formation/Formation-prise-de-poste

6.4 Constats et propositions du groupe de travail

442. La situation actuelle de la vidéoprotection dans un CSU est caractérisée par deux modes de fonctionnements qui influent sur le niveau de formation requis :

- Dans le premier dispositif, Il convient de préciser que certaines collectivités n'exploitent pas en temps réel les images qui sont donc simplement enregistrées et conservées durant la période légale de 30 jours maximum. Elles ne sont visualisées qu'à posteriori en cas de nécessité et sur réquisition des forces de l'ordre. Ainsi, plus de 99,99 % des images stockées ne sont donc jamais visionnées. Aucun personnel spécifique n'est alors affecté à ce dispositif consacré à la sécurisation des lieux publics.

- Dans le second dispositif, les images sont visualisées en temps réel au centre de supervision urbain. Elles requièrent donc un traitement immédiat et une organisation adéquate. Pour pouvoir correctement visionner des images, elles ne doivent pas être trop nombreuses. On considère qu'un vidéo opérateur installé dans un poste suffisamment ergonomique (environnement calme, lumière compatible, siège confortable, etc.) et muni de matériel d'utilisation simple et convivial, peut piloter de manière efficace une vingtaine de caméras maximum.

443. A ce jour, il n'existe aucun statut et déroulement de carrière dans de la fonction publique territoriale au métier d'opérateur vidéo. De fait, les agents sont recrutés sans critère véritablement objectifs. Ils possèdent des profils très différents d'une ville à l'autre : employés communaux, anciens policiers municipaux, emplois jeunes spécialisés dans la médiation et reconvertis pour l'occasion, anciens ASVP (Agent de surveillance de la voie publique).

444. Les municipalités ont souvent recours à du personnel reclassé (agents de service, assistantes maternelles, gardiens de musée, agents polyvalents) suite à des impératifs médicaux ou des raisons de service.

445. L'implication de ces opérateurs reclassés dans un service exempt de voie publique ou affectés par le fruit du hasard n'est pas forcement sujette à caution. Certains, extrêmement motivés, font même montre de compétences pointues.

446.Toutefois, il paraît essentiel que les centres de supervision urbains fonctionnent avec du personnel particulièrement motivé par la filière sécurité et spécifiquement formé à la vidéo. Faute de quoi, le risque d'avoir devant les écrans de simples téléspectateurs n'est pas négligeable. Sans motivation sécuritaire, l'opérateur ne sait quoi chercher, comment et sur quoi porter son attention. Il se contente de faire défiler des images, sans but précis.

447. L'emploi d'un personnel qualifié et réactif constitue une des conditions essentielles pour transformer la vidéo protection en une arme efficace en matière de lutte contre la délinquance.

448. Outre le statut, une autre question interpelle actuellement les collectivités. L'obligation de n'employer essentiellement et uniquement que des policiers municipaux dans les centres de supervision urbains reste onéreuse pour les collectivités territoriales.

449. Il paraît stratégique de privilégier le choix d'un cadre de la police municipale pour la direction d'un CSU intercommunal secondé par des chefs de salles aux grades de catégories C (brigadiers ou brigadiers chef principal) et dans les CSU communaux un ou des chefs de salles de catégorie C placés sous la responsabilité du responsable de la police municipale.

450. Ce personnel qualifié semble à même d'instiller la culture policière nécessaire aux opérateurs civils, notamment pour leur fixer des objectifs judiciaires, leur assigner des tâches précises, orienter leurs

recherches sur les comportements suspects… La présence dans le centre d'un agent assermenté et formé à la déontologie policière garantit, par ailleurs, une certaine éthique dans l'utilisation des images.

451. Il conviendrait peut être de créer un Cadre d'emploi du métier de vidéo-opérateur : OVP - opérateur-vidéo-Protection par la :

- Création d'une filière spécifique OVP calquée sur les 4 premières grilles de la catégorie C de la fonction publique territoriale.

- Mise en place d'un concours externe organisé par le CNFPT (dont les modalités resteront à définir) condition d'accès pour les candidats diplôme de niveau 5.

452. Ce cadre spécifique peut passer par la mise en place d'une épreuve orale en interne pour les agents titulaires de l'administration communale intéressés par le métier de vidéo-opérateur. Cette dernière serait composée d'un jury professionnel en matière de sécurité, afin de mieux détecter la fibre sécuritaire des postulants. Par ailleurs, l'avis de plusieurs personnes extérieures à la mairie permettra de limiter des reclassements d'office d'agents titulaires dans les CSU communaux ou intercommunaux.

453. A la réussite du concours ou de l'oral, les futurs OVP devraient suivre une formation obligatoire de vingt jours (cinq jours consacrés au volet juridique et quinze jours consacrés à la pratique) en partenariat avec le CNFPT qui devrait évaluer les compétences acquises et potentielles des candidats, ainsi que les obligations déontologiques liées à cette fonction.

454. Ce cadre serait également complété par la création d'une habilitation spécifique obtenue à l'issue de la formation initiale obligatoire. Elle pourrait être délivrée par le Procureur de la République sur proposition du maire et après une enquête des forces de l'ordre qui aurait pour objet de vérifier les conditions de moralités et d'honorabilité du futur OVP).

455. Cette assermentation devrait permettre aux vidéos-opérateurs civils encadrés par des policiers municipaux de procéder aux premiers recueils des éléments qui pourraient caractériser la commission d'une infraction grave au Code de la Route et à la Loi Pénale constatée en direct sur les écrans de vidéos-protection (vidéo-verbalisation - trafic de drogue - agression etc.) et dans le cadre du flagrant délit de pouvoir effectuer des relectures en liaison directe avec un OPJ ou APJ 20 sur le terrain pour les renseigner sur les éléments demandés.

Propositions du groupe de travail

- Créer un cadre d'emploi du métier de vidéo-opérateur : OVP - opérateur-vidéo-Protection :
  - Création d'une filière spécifique OVP calquée sur les 4 premières grilles de la catégorie C de la fonction publique territoriale.
  - Mise en place d'un concours externe organisé par le CNFPT (dont les modalités resteront à définir) condition d'accès pour les candidats diplôme de niveau 5.
  -

Ci-après une proposition d'adaptation des grilles de la catégorie C de la fonction publique territoriale pour prendre en compte le métier d'OVP.

Opérateur de Vidéo-Protection de 2ème classe (Catégorie C)

Echelon	Durée de l'échelon	IB	IM	Salaire brut
11	_	388	355	1643,75 €
10	36 à 48 mois	364	338	1565,04 €
9	36 à 48 mois	348	326	1509,48 €
8	36 à 48 mois	337	319	1477,06 €
7	36 à 48 mois	328	315	1458,54 €
6	24 à 36 mois	318	314	1453,91 €
5	24 à 36 mois	310	313	1449,28 €
4	24 à 36 mois	303	312	1444,65 €
3	18 à 24 mois	299	311	1440,02 €
2	18 à 24 mois	298	310	1435,39 €
1	12 mois	297	309	1430,76 €

Opérateur de Vidéo-Protection de 1ère classe (Catégorie C)

Echelon	Durée de l'échelon	IB	IM	Salaire brut
11	_	413	369	1708,58 €
10	36 à 48 mois	389	356	1648,38 €
9	36 à 48 mois	374	345	1597,45 €
8	36 à 48 mois	360	335	1551,15 €
7	36 à 48 mois	347	325	1504,84 €
6	24 à 36 mois	333	316	1463,17 €
5	24 à 36 mois	323	314	1453,91 €

Echelon	Durée de l'échelon	IB	IM	Salaire brut
4	24 à 36 mois	310	313	1449,28 €
3	18 à 24 mois	303	312	1444,65 €
2	18 à 24 mois	299	311	1440,02 €
1	12 mois	298	310	1435,39 €

Opérateur de Vidéo-Protection principal de 2ème classe (Catégorie C)

Echelon	Durée de l'échelon	IB	IM	Salaire brut
11	_	446	392	1815,07 €
10	36 à 48 mois	427	379	1754,88 €
9	36 à 48 mois	398	362	1676,17 €
8	36 à 48 mois	380	350	1620,60 €
7	36 à 48 mois	364	338	1565,04 €
6	24 à 36 mois	351	328	1518,74 €
5	24 à 36 mois	336	318	1472,43 €
4	24 à 36 mois	322	314	1453,91 €
3	18 à 24 mois	307	313	1449,28 €
2	18 à 24 mois	302	312	1444,65 €
1	12 mois	299	311	1440,02 €

Opérateur de Vidéo-Protection principal de 1ère classe (Catégorie C)

Echelon	Durée de l'échelon	IB	IM	Salaire brut
8	-	499	430	1991,03 €
7	36 à 48 mois	479	416	1926,20 €
6	36 à 48 mois	449	394	1824,33 €
5	24 à 36 mois	424	377	1745,62 €
4	24 à 36 mois	396	360	1666,91 €

Echelon	Durée de l'échelon	IB	IM	Salaire brut
3	18 à 24 mois	377	347	1606,71 €
2	18 à 24 mois	362	336	1555,78 €
1	18 à 24 mois	347	325	1504,84 €

7. Annexes

456.Liste des annexes :

- Glossaire des principaux termes du domaine
- Convention dispositif « Alertes commerçants » ville de Courcouronnes
- Liste des chartes éthiques étudiées
- Question parlementaire n° 85925, Réponse publiée au JO Ass. nat. du 23-8-2011
- Question parlementaire n° 45738, Réponse publiée au JO Ass. Nat. le 13-05-2014
- Question parlementaire n° n° 37524, Réponse publiée au JO Ass. Nat. le 11-03-2014
- Question parlementaire n° n° 37525, Réponse publiée au JO Ass. Nat. le 11-03-2014
- Liste des installateurs certifiés
- Fiches formations CNFPT, CNPP, GRETA, AFPA, AFPA et GPMSE
- Liste de principaux organismes
- Liste des membres du groupe de travail

7.1 Annexe 1 : Glossaire

Accès direct (stockage à) :

Cette notion réfère à la capacité d'un système de stockage à pouvoir accéder directement à une information enregistrée, sans parcourir l'enregistrement. Le système de stockage à accès direct le plus courant est le disque dur. Ces systèmes sont à opposer aux systèmes de stockage à accès séquentiel (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Accès séquentiel (stockage à) :

Stockage où la lecture et l'enregistrement s'effectuent selon un ordre prédéfini. Par exemple, les cassettes VHS, K7, DV, DAT, où, pour accéder à la troisième minute de l'enregistrement, il est nécessaire de parcourir les trois premières minutes, sont des systèmes de stockage à accès séquentiel (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Analogique :

Signal dans lequel chaque niveau est représenté par une tension électrique directement proportionnelle.

Pour les systèmes à enregistrement analogique des flux vidéo, un dispositif permet de déterminer à tout moment la date, l'heure et l'emplacement de la caméra correspondant aux images enregistrées (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Bande passante (réseau) :

Dans le domaine de l'informatique, le terme bande passante désigne un débit d'informations, plus précisément la quantité d'informations que peut transmettre un réseau (système informatique). Cette bande passante ce mesure généralement en octets par seconde ou en bits par seconde (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Caméra de vidéosurveillance :

Unité comportant un dispositif capteur d'image produisant un signal de vidéo provenant d'une image optique (Source : Norme NF EN 50312-7 décembre 2012 Systèmes d'alarme Surveillance CCTV usage applications sécurité Guidelines vidéoprotection).

Caméra de vidéosurveillance équipée :

Unité comportant une caméra de vidéosurveillance munie d'un objectif approprié et des matériels accessoires nécessaires (Source : Norme NF EN 50312-7 décembre 2012).

Caméra fixe :
Caméra attachée à un objet fixe (mur, lampadaire) permettant d'observer une aire donnée ou un périmètre prédéterminé lors de son installation. Elle n'est pas orientable.

Caméra orientable (Caméra PTZ) :
Caméra attachée à un objet fixe (mur, lampadaire) permettant d'observer une aire donnée ou un périmètre prédéterminé lors de son installation. Elle est orientable, et peut comporter un zoom et être capable d'observer des scènes à 360° pour en avoir une vision globale en permanence.

Ce type de caméra correspond à la Caméra PTZ définit comme une caméra à zoom et unité de panoramique et d'inclinaison (PTZ) sont des périphériques d'imagerie contrôlés par un opérateur ou un système de vidéosurveillance afin de modifier le champ de vision de la caméra à l'aide d'un moyen mécanique ou électronique. La caméra peut être dotée de l'une des fonctions ou d'une combinaison des fonctions de panoramique, d'inclinaison ou de zoom (Source : Norme NF EN 50312-7 décembre 2012).

Caméra mobile :
Caméra autonome portée par une personne « caméras piétons » (en général fixée sur un plastron ou sur un casque), déployée dans la zone publique d'un véhicule de transport collectif, installée temporairement à bord d'un véhicule et captant des images de la voie publique ou le domaine d'un réseau de transport guidé (*).

Note (*) Qu'elle soit fixe ou mobile, une caméra peut être :

- pilotée à distance depuis un ordinateur ou un mobile compatible.
- permanente lorsqu'elle fonctionne en continu ou qu'elle est fixée de façon permanente.
- temporaire lorsqu'elle ne fonctionne que pendant une ou plusieurs période ou qu'elle est installée à titre temporaire.

Caméra IP (ou caméra réseau) :

1) Les termes "caméra IP", "caméra réseau" et "caméra Internet" font tous référence à un même concept, à savoir une caméra et un ordinateur combinés au sein d'une même unité. Fonctionnant comme une unité indépendante, une caméra IP a juste besoin d'une connexion au réseau (Source : Lexique « Vidéo sur IP » Axis Communications).

2) Capteur traduisant l'image considérée en un ensemble de données numériques pouvant être stockées sur une unité d'archivage ad hoc (source : SNCF).

Cassettes VHS :

Support d'enregistrement analogique à accès séquentiel utilisant la norme VHS (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Centre de supervision urbain (CSU) :
Un centre de supervision urbain permet à une commune de rassembler en un même lieu les nouvelles technologies mises à disposition d'un service de police municipale et de visionner en temps réel les images transmises par les caméras de vidéoprotection.

Champ (optique) :
En optique, la notion de champ réfère à la portion d'espace visible à travers l'objectif de la caméra (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Commission départementale des systèmes de vidéosurveillance :
Commission administrative instituée dans chaque département chargée d'examiner les demandes d'installation de systèmes de vidéosurveillance (Code de la sécurité intérieure, art. L251-4).

Commission nationale de l'informatique et des libertés (CNIL) :
Autorité administrative indépendante chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Depuis la loi du 14 mars 2011, la Cnil exerce ses missions de contrôle des systèmes de vidéoprotection concurremment aux pouvoirs de contrôle dévolus à la commission départementale de vidéoprotection (Code de la sécurité intérieure, art. L253-2).

Commission nationale de la vidéoprotection (CNV) :
Autorité administrative qui exerce une mission de contrôle sur les conditions de fonctionnement d'un système de vidéoprotection, de conseil et d'évaluation de l'efficacité de la vidéoprotection. Elle émet des recommandations destinées au ministre de l'intérieur en ce qui concerne les caractéristiques techniques, le fonctionnement ou l'emploi des systèmes de vidéoprotection (Code de la sécurité intérieure, art. L253-1).

Compression :
1) Réduction de l'espace nécessaire au stockage et à la transmission de données (vidéos, images, etc.). Cette compression peut être réalisée avec ou sans perte d'information sur ces données (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17). Il existe différents types de codec (JPEG, MJPEG, MPEG, MPeg-2, MPEG-4, H.264, etc.).

2) Processus d'optimisation du poids numérique de l'image ayant pour objectif d'en faciliter le transport sur les réseaux et le stockage (source : SNCF).

Cybercaméra (n.f.) :
1) Caméra numérique, reliée à un ordinateur, qui permet de filmer et de diffuser en temps réel des vidéogrammes sur un réseau, en particulier l'internet. Équivalent étranger : webcam, webcaméra (Source : Vocabulaire de l'Audiovisuel, Journal officiel du 15 septembre 2006).

2) Caméra grand public autorisant l'archivage de données vidéo par l'intermédiaire d'un micro-ordinateur relié à l'internet.

Gyrocaméra (n.f.) :

1) Caméra aéroportée, stabilisée par un gyroscope. Note : « Wescam », qui est un nom de marque, ne doit pas être employé. Équivalent étranger : gyro-stabilized camera (Source : Vocabulaire de l'Audiovisuel, Journal officiel du 23 décembre 2007).

2) Caméra, dans le spectre du visible ou de l'invisible, stabilisée par un système gyroscopique (source : SNCF).

DAT :

Digital Audio Tape est à la base un support d'enregistrement audionumérique. Ce support est aujourd'hui également utilisé pour stocker des vidéos, de l'audio ou des données informatiques. Ce type de stockage est à accès séquentiel (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Déni de service :

En sécurité informatique, " l'attaque par déni de service " est une tentative de rendre une application, un système ou une ressource informatique indisponible à ses utilisateurs autorisés. Si un système informatique (serveur par exemple) n'est plus capable de traiter les requêtes de ses clients pour des raisons volontairement provoquées par un tiers, il y a " déni de service ". Le type d'attaque le plus répandu est de rendre un serveur inopérant en lui adressant de trop nombreuses requêtes. Les conséquences d'un tel acte peuvent se traduire dans le cas d'un système réseau de vidéoprotection par :

- un réseau inhabituellement ralenti (difficulté pour communiquer en continu avec une caméra par exemple) ;
- impossibilité d'accéder à une caméra particulière ;
- impossibilité d'accéder à n'importe quelle caméra ;
- augmentation du nombre de messages reçus via le réseau (mail, message de contrôle, message d'erreur, etc.) (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Disque dur :

Système de stockage à accès direct et à mémoire non volatile s'appuyant sur le principe de mémoire magnétique. Développé dans un premier temps pour une utilisation sur ordinateur, il a peu à peu remplacé tous les autres systèmes de stockage vidéo et audio par l'évolution rapide de sa capacité de stockage et de la facilité d'accès aux données sauvegardées (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Donnée à caractère personnel :

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne (Source : Loi n° 78-17 du 6 janvier 1978, art. 2).

Droit d'accès aux images :

Droit personnel d'accès aux enregistrements. Toute personne susceptible d'avoir été filmée dispose d'un droit d'accès aux images la concernant. L'exercice de ce droit est encadré par l'article L. 253-5 du Code de la sécurité intérieure.

Drone (n. m) :

1) Engin mobile, terrestre, aérien ou naval sans équipage, disposant de capacités de déplacement et navigation autonome et/ou télépilotée (Source : SNCF).

2) Aéronef télépiloté : aéronef qui circule sans personne à bord (Source : Arrêté du 11 avril 2012, NOR : DEVA1206042A)

A distinguer du drone de loisirs « aéromodèle » : aéronef télépiloté utilisé exclusivement à des fins de loisir ou de compétition par un télépilote qui est à tout instant en mesure de contrôler directement sa trajectoire pour éviter les obstacles et les autres aéronefs (Source : Arrêté du 11 avril 2012, NOR : DEVA1206042A).

Espace public :

1) L'espace public est constitué des voies publiques ainsi que des lieux ouverts au public ou affectés à un service public (Source : Loi n° 2010-1192 du 11 octobre 2010, art. 2).

2) La notion de voies publiques n'appelle pas de commentaire. Il convient de préciser qu'à l'exception de ceux affectés aux transports en commun les véhicules qui empruntent les voies publiques sont considérés comme des lieux privés. (…) Les commerces (cafés, restaurants, magasins), les établissements bancaires, les gares, les aéroports et les différents modes de transport en commun sont ainsi des espaces publics (Source : Circulaire du 2 mars 2011).

Etablissements ouverts au public :

Constituent des établissements recevant du public tous bâtiments, locaux et enceintes dans lesquels des personnes sont admises, soit librement, soit moyennant une rétribution ou une participation quelconque, ou dans lesquels sont tenues des réunions ouvertes à tout venant ou sur invitation, payantes ou non. Sont considérées comme faisant partie du public toutes les personnes admises dans l'établissement à quelque titre que ce soit en plus du personnel (Source : Code de la construction et de l'habitation : art. R123-2).

Exportation (de données) :

Opération consistant à copier ou à extraire du système de stockage des informations ciblées (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Fichier de données à caractère personnel :

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés (Source : Loi n° 78-17 du 6 janvier 1978, art. 2).

Fichier "DRACAR" :

Le fichier DRACAR est un outil de gestion des préfectures et du CNAPS (Conseil national des activités privées de sécurité). Traitement automatisé de données à caractère personnel relatif à la carte professionnelle des agents de sécurité privée dénommé « DRACAR » ayant pour finalité d'attribuer, si les conditions légales sont respectées :

1° Un numéro de carte professionnelle délivrée aux personnes souhaitant être employées pour participer à une activité mentionnée à l'article 1er de la Loi 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité ;

2° Un numéro d'autorisation préalable ou d'autorisation provisoire délivrée aux personnes souhaitant se former aux fins d'acquérir l'aptitude professionnelle nécessaire à l'obtention de la carte professionnelle (Source : Arrêté du 9 février 2009 modifié par l'arrêté du 8 juin 2012).

Fichier "Téléc@artepro" :

Traitement automatisé de données à caractère personnel dénommé « Téléc@rtepro » qui prend la forme d'un téléservice ayant pour finalité de permettre :
— aux employeurs des sociétés de sécurité privée et des agences de recherches privées de vérifier que les candidats à l'embauche ou leurs salariés sont titulaires d'un numéro de carte professionnelle ou d'autorisation provisoire délivrées par le préfet ou le Conseil national des activités privées de sécurité, en cours de validité ;
— aux clients des sociétés de sécurité privée et des agences de recherches privées de vérifier que ces sociétés et agences sont autorisées à exercer, que leurs dirigeants sont agréés et que leurs agents disposent d'une carte professionnelle, en cours de validité ;
— aux personnes susceptibles d'être employées par les sociétés de sécurité privée et agences de recherches privées de vérifier que ces sociétés et agences sont autorisées à exercer leur activité ;
— aux organismes de formation de vérifier que les candidats à la formation sont titulaires d'un numéro d'autorisation préalable délivrée par le préfet ou le Conseil national des activités privées de sécurité, en cours de validité » (Source : Arrêté du 9 février 2009 modifié par l'arrêté du 8 juin 2012).

Flux :

1) En informatique, ensemble de données élémentaires issues d'un système informatique (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

2) Ensemble de données informatiques acheminées par un réseau de transport dont le traitement concourt à l'affichage sur un terminal de visualisation (Source SNCF).

Focale (distance) :

La distance focale d'un système optique est l'une des grandeurs qui définit entièrement un système optique. On peut l'assimiler dans la plupart des cas à la distance entre l'objectif et le capteur de la caméra (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Format CIF (4 CIF) (*Common Intermediate Format*) **:**

Le format CIF est un format numérique d'images de 352 x 288 pixels. Le format 4 CIF évoqué dans cette circulaire est le format d'image standard de 704 x 576 pixels (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Format d'image :

Taille de l'image définie en terme de pixels ou de lignes et de colonnes (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Installateur :

Entreprise qui installera le système, suite à un contrat avec le maître d'ouvrage. Dans la mesure où l'autorisation délivrée par les préfectures est une autorisation préalable, l'installateur n'est en général que pressenti (suite à un devis), voire n'est pas encore connu (cas d'un appel d'offres) (Source : Arrêté du 5 janvier 2011, annexe sur les conditions requises pour la certification des installateurs de systèmes de vidéosurveillance par un organisme accrédité, NOR : OCD1033809A).

Installation de vidéosurveillance :

Installation comprenant les composants matériels et logiciels d'un système de vidéosurveillance, installés et fonctionnant en totalité, pour surveiller une zone de sécurité définie (Source : Norme NF EN 50312-7 décembre 2012).

Parmi les exigences minimales à respecter par les installateurs pour obtenir la certification, figure notamment l'obligation de proposer un contrat de maintenance au maître d'ouvrage (ce dernier n'étant pas tenu de l'accepter) (Source : Arrêté du 5 janvier 2011 abrogeant l'arrêté du 29 avril 2010).

Interopérabilité :

Capacité pour des équipements ou des systèmes d'origines diverses (constructeurs ou éditeurs différents) à fonctionner harmonieusement au sein d'un même système global.

Dans le cas de la vidéo surveillance, chaque constructeur de caméra implémente ses propres algorithmes de compression et ses propres méthodes de renseignement des métadonnées (horodatage, positionnement, mouvement, couleur, etc.). Il n'existe à l'heure actuelle aucune norme définissant un mode opératoire unique. Le but d'une image ou d'une séquence vidéo étant essentiellement de pouvoir être retrouvée, identifiée et relue par un tiers, il est indispensable que toutes les interfaces propriétaires soient accessibles, en attendant qu'une norme technique soit publiée et implémentée. La conformité à des standards en cours de développement tels qu'Onvif ou PSIA[104] constitue une base de travail, mais ne permet pas de garantir de manière absolue l'interopérabilité entre les différents éléments constituant un système de vidéo surveillance (source : Garry Goldenberg, président du forum Open IP Video).

IP (*Internet protocol*) **:**

1) Utilisation du réseau Internet pour transmettre les images à l'enregistreur, grâce à l'adresse IP - L'images reçue peut alors être visible sur n'importe quel matériel relié à Internet (Smartphone, Ordinateur, Tablettes, etc.)

2) Processus d'échanges de données entre différents équipements de nature numérique fondé sur les protocoles utilisés sur l'internet (Source SNCF).

Liaison logicielle :

Liaison assurée par un logiciel informatique de manière automatique entre plusieurs données ou opérateurs (Source : Arrêté du 3 août 2007 modifié par la loi 2011-267 du 14 mars 2011 - art. 17).

Lieux affectés à un service public :

Les lieux affectés à un service public désignent les implantations de l'ensemble des institutions, juridictions et administrations publiques ainsi que des organismes chargés d'une mission de service public. Sont notamment concernés les diverses administrations et établissements publics de l'Etat, les collectivités territoriales et leurs établissements publics, les mairies, les tribunaux, les préfectures, les hôpitaux, les bureaux de poste, les établissements d'enseignement (écoles, collèges, lycées et universités), les caisses d'allocations familiales, les caisses primaires d'assurance maladie, les services de Pôle emploi, les musées et les bibliothèques (Source : Circulaire du 2 mars 2011).

[104] Onvif (Open Network Video Interface Forum) http://www.onvif.org/ et PSIA (Physical Security Interoperability Alliance) http://www.psialliance.org/ sont deux initiatives industrielles concurrentes pour définir un standard de communication entre équipements de vidéosurveillance et contrôle d'accès.

Lieux ouverts au public :

1) Constituent des lieux ouverts au public les lieux dont l'accès est libre (plages, jardins publics, promenades publiques, commerces, etc.) ainsi que les lieux dont l'accès est possible, même sous condition, dans la mesure où toute personne qui le souhaite peut remplir cette condition (paiement d'un droit d'entrée, par exemple au cinéma) (Source : Circulaire du 14 septembre 2011).

2) Un lieu ouvert au public est un lieu pour lequel il n'existe pas de restriction d'accés. Le simple paiement d'une somme d'argent n'est pas considéré comme constituant une restriction d'accés. Ainsi les commerces, les cinémas, les restaurants, les services publics recevant des usagers, les parcs d'attraction sont considérés comme des lieux ouverts au public (Source SNCF).

Lieux privés / lieux non ouverts au public :

1) Sont considérés comme des lieux non ouverts au public, les parties communes des immeubles d'habitation, les locaux professionnels et les établissements affectés à l'enseignement ou à la garde d'enfants (Source : Circulaire du 14 septembre 2011).

2) Au terme d'une jurisprudence constante[105], un lieu privé est un lieu où quiconque ne peut pénétrer ou accéder sans le consentement de l'occupant, peu important que ce lieu se trouve inclus dans un bâtiment ouvert au public.

3) Constitue un lieu non ouvert au public celui pour lequel il existe une restriction d'accés. Ainsi les bureaux d'un organisme public ou privé, les réserves et autres locaux dédiés au personnel sont des lieux non ouverts au public (Source SNCF).

Maître d'ouvrage :

Entité qui est responsable de la mise en place d'un système de vidéoprotection (collectivité locale, supermarché, banque, etc.). Le maître d'ouvrage peut s'engager à prendre un installateur titulaire d'un certificat délivré par un organisme certificateur, afin de bénéficier de la procédure simplifiée d'autorisation en préfecture (Source : Arrêté du 5 janvier 2011, annexe sur les conditions requises pour la certification des installateurs de systèmes de vidéosurveillance par un organisme accrédité, NOR : OCD1033809A).

[105] Cass. crim., 16 février 2010, pourvoi n°09-81492, Bull. crim. 2010, n° 25 (rejet) ; Cass. crim., 25 avril 1989, pourvoi n° 86-93632, Bull. crim. 1989, n° 165 (rejet) ; Cass. crim., 12 avril 2005, pourvoi n° 04-85637, Bull. crim. 2005, n° 122 (cass. partielle) ; Cass. crim., 14 février 2006, pourvoi, n° 05-84384, Bull. crim. 2006, n° 38 (rejet).

7.2 Annexe 2 : Convention dispositif « Alerte commerçants »

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONVENTION

DISPOSITIF « ALERTE COMMERCANTS »

POLICE MUNICIPALE

ENTRE LES SOUSSIGNES

La **Ville de COURCOURONNES**, représentée par Stéphane BEAUDET, Maire de Courcouronnes agissant ès qualités en vertu de la délibération du Conseil Municipal en date du 27 juin 2013,

Ci-après dénommée « **la Ville** »

ET

M. ou Mme ....., propriétaire du commerce dénommé « ..... », Société .....au capital de ..... €, immatriculée au Registre du Commerce et des Sociétés de .....sous le numéro....., dont le siège social est à .....,
Représentée par M. ou Mme ....., en qualité de ....., dûment habilité à l'effet des présentes,

Ci-après dénommée « **le commerçant** »

Ci- après désignés « **la ou les Partie(s)** »

IL EST D'ABORD EXPOSE CE QUI SUIT :

Devant la recrudescence des agressions et des braquages à l'encontre des commerçants des quartiers du Centre et du Canal, la ville de Courcouronnes a décidé de mieux sécuriser les commerces de proximité en proposant la création et la mise en place d'un système d'alerte pour les commerçants.

Ce dispositif est relié directement au poste de la Police Municipale, par l'utilisation de nouvelles technologies de communication, pour :

•permettre l'information immédiate, rapide et discrète au CSU de la police municipale

•et faciliter la sécurité et l'efficacité d'une éventuelle intervention des polices (nationale-municipale).

La présente convention a donc pour objet de définir les engagements réciproques consentis entre les parties dans le cadre de la mise en place de ce système d'alerte et de protection.

IL A ETE CONVENU CE QUI SUIT :

ARTICLE 1 - OBJET

Par la présente convention d'usage, la Ville de Courcouronnes accepte que M. ou Mme ....., propriétaire du commerce, sus dénommé « ..... », soit connecté directement au PC de la Police Municipale au moyen d'un système d'alerte et de protection, conforme aux dispositions de l'article 2, cité ci-dessous.

ARTICLE 2 - LES DEUX TECHNOLOGIES PROPOSÉES

1/ Alerte par transmetteur téléphonique avec émetteur pendentif

Le transmetteur téléphonique Vocalys AS installé chez le commerçant est raccordé au poste de la Police Municipale, par ligne téléphonique, sur un PC dédié à cette fonction. En cas d'urgence, le commerçant déclenche l'alarme en appuyant soit :

•sur le bouton rouge du transmetteur dissimulé à proximité de la caisse,

•soit au moyen du pendentif qu'il peut porter sur lui, d'une portée de 150 mètres.

Aussitôt, la Police Municipale reçoit l'appel d'urgence dans les 20 secondes sur le PC avec les coordonnées du commerce, avec la possibilité d'écouter les faits se produisant à l'intérieur du commerce ; puis 10 secondes plus tard, sur le portable de patrouille sous forme d'un SMS, signalant le lieu de l'alarme.

2/ Alerte par vidéo-protection

Les nouvelles technologies nous permettent de moderniser notre système et de proposer la protection des commerçants par vidéo-protection reliée directement au Centre de Supervision Urbaine (CSU) de la Police Municipale.

En cas de déclenchement de l'alerte par pression sur le bouton ou sur le pendentif que le commerçant porte sur lui, le vidéo-opérateur reçoit une sirène pour l'alerter du SOS et la visualisation du commerce sur l'écran est instantanée (selon les caméras installées à l'intérieur du commerce).

Le vidéo-opérateur peut observer et entendre ce qui se passe dans le commerce en direct :

•soit le commerçant est victime d'un braquage ou d'une agression, alors les forces de l'ordre sont immédiatement alertées,

•soit il ne constate aucun problème et prendra contact téléphoniquement avec le commerçant pour connaître le motif du déclenchement de l'alerte.

ARTICLE 3 - LE PRINCIPE DU SYSTEME

Le dispositif « alerte commerçant » est un moyen de prévention complémentaire à la vidéo-protection de la ville. Il est signalé à l'entrée du commerce par une affichette avec les inscriptions suivantes : «***Attention - commerce protégé par vidéo-protection relié directement à la police municipale, pour tout incident, l'intervention des forces de l'ordre est immédiate*** ».

Ce support d'information est fourni par la ville et le commerçant devra l'apposer sur sa vitrine de manière à ce qu'elle soit bien visible du public. Il a également pour objectif de rassurer les employés, la clientèle et de dissuader le délinquant de passer à l'acte, en le rendant plus compliqué, voire risqué.

ARTICLE 4 - MODALITES FINANCIERES

L'acquisition et la maintenance du matériel selon les deux technologies proposées par plusieurs prestataires sont à la charge du commerçant.

Si ce dernier choisit :

•la vidéo-protection : son installation s'effectuera par des techniciens de la société choisie. Ensuite ces derniers se mettront en relation avec le CSU de la Police Municipale pour paramétrer les connections.

•le transmetteur téléphonique (dès son acquisition par le commerçant) : son installation, paramétrage et sa connexion au CSU de la Police Municipale seront assurés par un agent du service formé à cette technologie.

La ville prend en charge l'acquisition du logiciel et de sa maintenance. Ce dispositif n'engage aucun abonnement du commerçant et les interventions de la police municipale sont effectuées dans le cadre de la sécurité publique et de la protection des commerces de proximité.

Tous les dégâts et dégradations survenues aux installations du commerçant seront à la charge de celui-ci.

Le commerçant s'engage à effectuer à ses frais, risques et périls et à sa diligence, toutes les réparations, de façon à ce que l'ensemble du matériel demeure toujours viable pour assurer une liaison permanente avec le Centre de Protection Urbaine de Cannes. Dès lors, la responsabilité de la Ville de Courcouronnes ne peut être utilement recherchée à l'occasion d'un matériel défectueux.

Pendant toute la durée de la présente convention, la Ville de Courcouronnes fera son affaire personnelle et prendra en charge l'entretien de ses propres réseaux afin d'assurer au commerçant une liaison permanente avec le Centre de Protection Urbaine.

ARTICLE 5 - OBLIGATIONS DE LA POLICE MUNICIPALE

Lorsque l'alerte sera actionnée par le commerçant, la police municipale s'engage à :

- **prévenir** immédiatement le PC de la Police Nationale par le biais de la fibre optique ;
- **analyser** la situation par la vidéo-protection ou par l'écoute téléphonique du commerce ;
- **intervenir**, dans les plus brefs délais, auprès du commerçant aux heures s'échelonnant de l'ouverture à la fermeture incluse du magasin ;
- **tester** une fois par semaine le bon fonctionnement du système ; et durant les périodes à risque, une fois par jour (soldes et fêtes de fin d'année) ;
- **assurer** une astreinte téléphonique le samedi matin et le dimanche toute la journée pour les commerçants ouverts pendant cette période ;

Cela signifie que, si le commerçant déclenche l'alerte, le SOS sera transféré sur le portable d'astreinte de la Police Municipale, qui préviendra immédiatement la Police Nationale pour une intervention dans les plus brefs délais.

ARTICLE 6 - OBLIGATIONS DU COMMERCANT

Le commerçant s'engage à respecter les obligations suivantes :

- **afficher** à l'entrée de son commerce le support informant de l'existence du dispositif «*alerte commerçants* » de manière à ce qu'il soit bien visible du public ;
- **déclencher** l'alerte uniquement en cas d'agression, de vol à main armée ou d'un fait grave à proximité du commerce ;
- **prévenir** la police municipale, dans les plus brefs délais, en cas de déclenchement intempestif pour annuler l'intervention de police au numéro suivant : 06-10-17-33-22, le numéro de téléphone est également indiqué sur le transmetteur téléphonique.

Chaque déclenchement de l'alerte entraînera une intervention prioritaire de la police municipale qui sera immédiatement en relation avec la police nationale d'Évry.
Pour tout autre événement sur la voie publique, le commerçant devra composer le 17 ou la ligne directe de la Police municipale.

ARTICLE 7 - RESPONSABILITES

Par la présente convention, la Ville de Courcouronnes ne peut garantir qu'une obligation de moyens et sa responsabilité ne saurait alors être engagée pour tous faits ou dommages que ce soient, notamment en cas de vol à main armé ou d'agression physique.
Il est précisé que les compagnies d'assurances renoncent à tous recours contre la Ville dès lors que cette dernière se place dans l'exécution de la présente convention.
Pour une parfaite compréhension des présentes, il est précisé que le dispositif « Alerte Commerçant » n'a pas la fonction de signaler une intrusion ou un cambriolage en cours. Cependant, si la police municipale est contactée par le chef des lieux ou une société privée de gardiennage suite au déclenchement de l'alarme du commerce, elle interviendra au même titre qu'un appel d'un tiers ou en flagrant délit.

Le commerçant s'engage à effectuer à ses frais, risques et périls et à sa diligence, toutes les réparations, de façon à ce que l'ensemble du matériel demeure toujours viable pour assurer une liaison permanente avec le PC de la Police Municipale.
Dès lors, la responsabilité de la Ville de Courcouronnes ne peut être utilement recherchée à l'occasion d'un matériel défectueux, d'une panne technique due à une coupure de courant ou de téléphone ou tout autre dysfonctionnement n'ayant aucune incidence avec le logiciel de la police municipale.

ARTICLE 8 - INFORMATIQUE ET LIBERTES

Le commerçant est informé que les données fournies sont intégrées à un fichier informatisé dûment déclaré à la CNIL par la ville de Courcouronnes ; celles-ci ne seront utilisées qu'aux seules fins du dispositif d'alerte mis en place par la ville de Courcouronnes.

Conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il dispose d'un droit d'accès et de rectification des données le concernant, en écrivant par simple lettre au Directeur de la Police Municipale.

ARTICLE 9 - DUREE DE LA CONVENTION

La présente convention prendra effet dès notification par la Ville de Courcouronnes de la présente, signée, paraphée et revêtue du visa du contrôle de légalité, garantissant ainsi tout effet exécutoire.

La présente convention est conclue pour une durée d'**1 an**.

A l'expiration de cette dernière, la présente convention sera reconduite annuellement par tacite reconduction dans la limite d'une durée totale de **12 ans**.

ARTICLE 10 - RESILIATION

Chacune des deux parties aura la faculté de mettre un terme à la présente convention par lettre recommandée avec accusé de réception adressée à l'autre au moins 1 mois à l'avance.

ARTICLE 11 - LITIGES

Tout différend ou conflit entre les parties portant sur la validité, l'interprétation ou l'exécution de la présente convention fera l'objet d'une tentative de règlement amiable entre les parties préalablement à toute action judiciaire.

A défaut d'accord amiable, le différend sera porté par la partie la plus diligente devant le Tribunal administratif de Versailles, seul compétent.

ARTICLE 12 - ELECTION DE DOMICILE

Pour l'exécution de la présente convention, les parties élisent domicile en leurs sièges respectifs. Toute convention, notification ou avenant ultérieur devra être fait à ces adresses, sauf changement dûment notifié à l'autre partie.

Fait à Courcouronnes, le .....,
en deux exemplaires,

Pour la Ville de Courcouronnes

Pour M. ou Mme .....
« Commerçant »

7.3 Annexe 3 : Liste des chartes éthiques étudiées

Charte d'éthique de la vidéoprotection Ville de Paris :
http://www.prefecturedepolice.interieur.gouv.fr/content/download/3132/14772/file/Charte%20d'%C3%A9thique%20de%20la%20vid%C3%A9oprotection%20%C3%A0%20Paris.pdf

Charte déontologique de la vidéosurveillance Ville de Clichy:
http://owni.fr/files/2011/12/fichier_charte1_518.pdf

Charte d'éthique de la vidéosurveillance Ville de Lyon :
http://www.static.lyon.fr/vdl/contenu/securite/charteEthiqueVideosurveillanceLyon.pdf

Charte d'éthique et d'évaluation de la Vidéosurveillance municipale Ville de Rouen :
http://www.rouen.fr/sites/default/files/charte-video.pdf

Charte d'éthique de la vidéosurveillance Ville de Sénart :
http://www.senart.com/fileadmin/SENART/MEDIA/vie_pratique/securite/CharteEthiqueVideoprotectionSenart_Signee.pdf

Charte d'éthique de la vidéosurveillance Ville de Saint Benoit :
http://www.ville-saint-benoit.fr/uploads/assets/chartevideosaintbenoit_170611_4e1b0a8f76680.pdf

Charte d'éthique de la vidéosurveillance Ville de Hayange :
http://www.ville-hayange.fr/medias/charte_videoprotection.pdf

Charte d'éthique de la vidéosurveillance Ville de Lure :
Communauté de commune du pays de Lure

Charte d'éthique de la vidéosurveillance Ville d'Argenteuil :
http://www.argenteuil.fr/uploads/Document/13/2286_1297970581_CHARTE_VIDEOSURVEILLANCE.pdf

7.4 Annexe 4 : Questions parlementaires

7.4.1 Question N° 85925, Réponse publiée au JO Ass. nat. du 23-8-2011

ASSEMBLÉE NATIONALE

Sauvegarder en pdf Imprimer

13ème législature

Question N° : 85925	de M. Jean-Claude Mignon (Union pour un Mouvement Populaire - Seine-et-Marne)	Question écrite

Ministère interrogé > Justice et libertés (garde des sceaux)	Ministère attributaire > Justice et libertés

Rubrique > sécurité publique	Tête d'analyse > sécurité des biens et des personnes	Analyse > Commission nationale de vidéosurveillance. missions

Question publiée au JO le : 03/08/2010 page : 8466
Réponse publiée au JO le : 23/08/2011 page : 9179
Date de changement d'attribution : 14/11/2010

Texte de la question

M. Jean-Claude Mignon appelle l'attention de Mme la ministre d'État, garde des sceaux, ministre de la justice et des libertés, sur le nécessaire contrôle des dispositifs de vidéosurveillance. La vidéosurveillance est devenue en quelques années un outil privilégié de la lutte contre la délinquance. Son succès n'exclut pourtant pas de rester vigilant sur certaines dérives potentielles pouvant porter atteintes aux libertés fondamentales. La législation existante offre, il est vrai, des garanties dans ce domaine en limitant, par exemple, la durée de conservation des enregistrements, en obligeant à identifier clairement le responsable du système de vidéosurveillance ou encore en permettant aux personnes concernées un accès aux enregistrements visuels. Toutefois, contrairement à d'autres pays européens et malgré les préconisations de plusieurs rapports d'information parlementaire récents, la France ne dispose pas d'autorité indépendante pouvant superviser le contrôle de ces dispositifs sur l'ensemble du territoire national, harmoniser les pratiques et en évaluer l'efficacité. Afin de mettre à profit les institutions existantes et éviter ainsi la création d'une autorité nouvelle, ces prérogatives pourraient être confiées à la Commission nationale de l'informatique et des libertés ou à la commission nationale de vidéosurveillance dont le rôle est aujourd'hui purement consultatif. Il souhaite, par conséquent, connaître les intentions du Gouvernement sur cette question.

Texte de la réponse

En application de l'article 10 de la loi du 10 janvier 1995 d'orientation et de programmation relative à la sécurité, l'autorisation d'installer un système de vidéoprotection relève de deux régimes juridiques différents : la Commission nationale de l'informatique et des libertés se prononce sur les systèmes installés dans les lieux publics dont les enregistrements sont utilisés dans des traitements structurés permettant l'identification des personnes ; les autres systèmes sont autorisés par le représentant de l'État, après avis de la commission départementale de vidéoprotection. Depuis la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, modifiant l'article 10 de la loi du 10 janvier 1995 précitée, le contrôle a posteriori du système de vidéoprotection est également soumis à un double régime juridique. Lorsque l'installation du dispositif a été autorisée par le représentant de l'État dans le département, ou le préfet de police à Paris, le pouvoir de contrôle de ces installations relève de la commission départementale de vidéoprotection compétente. Celle-ci peut, à tout moment, contrôler les conditions de fonctionnement du dispositif, à savoir notamment les éléments relatifs à l'enregistrement et à la durée de conservation des images. Elle émet, le cas échéant, des recommandations et propose la suspension ou la suppression des dispositifs non autorisés, non conformes à leur autorisation ou dont il est fait un usage anormal. Elle informe le maire de la commune concernée. En revanche, si la mise en oeuvre d'un tel système a été autorisée par la Commission nationale de l'informatique et des libertés, celle-ci dispose de l'intégralité de son pouvoir d'enquête et de sanction, afin de s'assurer du respect de la déclaration ou de l'autorisation effectuée pour les enregistrements. Par ailleurs, la Commission nationale de l'informatique et des libertés peut, sur demande de la commission départementale compétente, du responsable d'un système ou de sa propre initiative, exercer un contrôle visant à s'assurer que le système est utilisé conformément à son autorisation et, selon le régime juridique dont le système relève, aux dispositions de la loi du 10 janvier 1995 susvisée ou à celles de la loi du 6 janvier 1978 modifiée. Lorsque la Commission nationale de l'informatique et des libertés constate un manquement aux dispositions de la loi du 10 janvier 1995 susvisée, elle peut, après avoir mis en demeure la personne responsable du système de se mettre en conformité, dans un délai qu'elle fixe, demander au représentant de l'État dans le département et, à Paris, au préfet de police, d'ordonner la suspension ou la suppression du système de vidéoprotection. Elle informe le maire de la commune concernée de cette demande.

7.4.2 Question n° 45738, Réponse publiée au JO Ass. Nat. le 13-05-2014

ASSEMBLÉE NATIONALE

14e législature		
Question n° : 45738	**de M. Rémi Delatte (Union pour un Mouvement Populaire - Côte-d'Or)**	**Question écrite**
Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur	
Rubrique > police	**Tête d'analyse** > police municipale	**Analyse** > caméras individuelles portées. mise en oeuvre. réglementation
Question publiée au JO le : **10/12/2013** page : **12829** Réponse publiée au JO le : **13/05/2014** page : **3898** Date de changement d'attribution : **03/04/2014**		

Texte de la question

M. Rémi Delatte interroge M. le ministre de l'intérieur sur la réglementation des caméras-piéton pour les policiers. Depuis quelques temps la police nationale et la gendarmerie testent les caméras-piéton sur leurs agents lors d'interventions difficiles. La caméra est déclenchée par l'agent quand il estime que l'intervention devient conflictuelle tant sur la voie publique que dans les lieux privés où il intervient. L'agent en averti l'intéressé. Les collectivités territoriales s'interrogent sur les autorisations à solliciter et les textes réglementaires à respecter avant de mettre cet outil à disposition de leur police municipale. La réglementation de 1995 concerne la vidéoprotection urbaine et la vidéoprotection dans le cercle privé, notamment les commerces. Cependant aucun texte ne précise pour ce type d'équipement les démarches à entreprendre auprès de la CNIL ou de la préfecture, ni la durée de sauvegarde des images, de leurs exploitations ou droit d'accès. Il souhaite connaître la réglementation qui s'applique aux caméras-piéton portées dans le cadre de leurs missions par les policiers municipaux.

Texte de la réponse

Plusieurs actions ont été récemment entreprises pour améliorer les relations entre les forces de l'ordre et la population : ouverture au public d'une plate-forme internet de signalement des manquements déontologiques gérée par l'inspection générale de la police nationale, nouveau code de déontologie commun aux policiers et aux gendarmes, numéro d'identification sur l'uniforme des policiers et gendarmes. Dans ce contexte, les « caméras-piéton » visent à sécuriser les interventions de voie publique, tout particulièrement lors des contrôles d'identité. En effet, les forces de l'ordre sont soumises à des agressions de plus en plus violentes et leur action est régulièrement contestée ou dénaturée. Les images issues de la caméra constituent alors un élément de preuve sur les conditions d'intervention. Une expérimentation de « caméras-piéton », réservées aux seuls personnels en uniforme de la gendarmerie nationale et de la police nationale, a été initiée dans plusieurs zones de sécurité prioritaire (ZSP) et dans des quartiers dits « sensibles ». A la fin de l'année 2013, 238 caméras étaient affectées dans les services de police dans ces ZSP et 528 en zone gendarmerie. A l'issue de cette expérimentation, qui s'inscrit d'ores-et-déjà dans le cadre des dispositions relatives au droit au respect de la vie privée (articles 9 du code civil et 226-1 du code pénal), le cadre juridique d'emploi des « caméras-piétons » sera précisé. Un suivi régulier des retours d'expérience des utilisateurs est assuré par un comité de pilotage réunissant les services centraux et les services opérationnels. Le premier bilan d'utilisation est positif car les relations entre les utilisateurs et les personnes contrôlées sont plus apaisées dans les zones de déploiement. Cette utilisation expérimentale est réservée aux seuls fonctionnaires de police et militaires de la gendarmerie nationales dans la mesure où les contrôles d'identité relèvent de leur compétence.

7.4.3 Question n° 37524, Réponse publiée au JO Ass. Nat. le 11-03-2014

ASSEMBLÉE NATIONALE

14e législature		
Question n° : 37524	**de Mme Fanélie Carrey-Conte (Socialiste, républicain et citoyen - Paris)**	**Question écrite**
Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur	
Rubrique > ordre public	**Tête d'analyse** > maintien	**Analyse** > caméra-piéton. expérimentation. évaluation
Question publiée au JO le : **17/09/2013** page : **9597** Réponse publiée au JO le : **11/03/2014** page : **2424**		

Texte de la question

Mme Fanélie Carrey-Conte interroge M. le ministre de l'intérieur sur le dispositif d'expérimentation de "cameras-piétons" mis en œuvre par la police à Nîmes. Elle souhaiterait obtenir des détails sur le fonctionnement précis de ce dispositif. Elle aimerait notamment savoir si les fonctionnaires de police déclencheront les caméras à chaque fois qu'ils auront une interaction avec une personne ou s'ils disposeront d'une marge discrétionnaire en la matière, et si les policiers ont reçu des instructions précises pour les aider dans ces décisions. D'autre part, elle souhaiterait connaître la méthode d'évaluation de ce dispositif. Cette mesure ayant été présentée comme une manière de lutter contre les contrôles au faciès, elle aimerait notamment savoir comment l'expérimentation permettra de vérifier si cet objectif est atteint.

Texte de la réponse

Plusieurs actions ont été entreprises pour renforcer les liens des forces de l'ordre avec la population : ouverture au public d'une plate-forme internet de signalement des manquements déontologiques, nouvelles règles déontologiques applicables aux contrôles d'identité et aux palpations de sécurité, évolution en profondeur de la formation des policiers et des gendarmes, ou encore, publication d'une nouvelle version du code de déontologie. Des policiers et des gendarmes mieux respectés et plus proches de la population sont, en effet, plus efficaces. Les caméras-piéton participent de cette logique : professionnaliser et dépassionner les interventions en favorisant la désescalade de la tension, sécuriser les interventions de voie publique des policiers en les objectivant. La caméra constitue en effet un élément de preuve irréfutable sur les conditions d'intervention. Depuis l'automne 2012, une expérimentation de caméras-piéton a été initiée dans plusieurs zones de sécurité prioritaires (ZSP), réservés à des fonctionnaires de police et ds militaires de la gendarmerie travaillant en tenue d'uniforme. A compter de mai 2013, 205 caméras ont ainsi été affectées dans les services de police et unités de gendarmerie compétentes dans les ZSP. S'agissant d'une expérimentation, leur doctrine d'emploi n'est pas encore fixée de manière précise et définitive. Il doit toutefois être souligné que ces caméras n'ont pas à ce stade vocation à filmer des lieux privés. Le cadre juridique est en effet à l'étude pour déterminer les conditions d'emploi des caméras-piéton (enregistrement de toutes les interventions ou des seules situations à risque...consentement des personnes filmées...), la nature des lieux dans lesquels un enregistrement peut être réalisé (lieu public, lieu privé ouvert ou non au public...) et la durée de conservation des données (images et sons). Un projet d'arrêté-cadre relatif au dispositif des caméras est en préparation. Un suivi régulier de l'expérimentation, à partir des retours d'expériences des utilisateurs, est assuré par un comité de pilotage réunissant au niveau central (direction générale de la police nationale) les services techniques et les services opérationnels. Cette instance s'est déjà réunie à quatre reprises. D'ores et déjà, le premier bilan d'utilisation est positif, puisque l'objectif principal est atteint : les caméras « pacifient » les relations entre les utilisateurs et les personnes contrôlées. Par ailleurs, les images et le son sont de très bonne qualité.

7.4.4 Question n° 37525, Réponse publiée au JO Ass. Nat. le 11-03-2014

ASSEMBLÉE NATIONALE

14e législature		
Question n° : 37525	**de Mme Fanélie Carrey-Conte (Socialiste, républicain et citoyen - Paris)**	**Question écrite**
Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur	
Rubrique > ordre public	**Tête d'analyse** > maintien	**Analyse** > caméra-piéton. expérimentation. évaluation
Question publiée au JO le : **17/09/2013** page : **9598** Réponse publiée au JO le : **11/03/2014** page : **2424**		

Texte de la question

Mme Fanélie Carrey-Conte interroge M. le ministre de l'intérieur sur le dispositif d'expérimentation de "cameras-piétons" mis en œuvre par la police à Saint-Denis ainsi qu'à Saint-Étienne. Elle souhaiterait plus d'informations sur ces expériences, sur quelle période et dans quelles zones elles ont été mises en place. Elle demande qui a évalué les résultats de ces expérimentations, suivant quelle méthodologie d'évaluation, et quels en ont été les résultats.

Texte de la réponse

Plusieurs actions ont été entreprises pour renforcer les liens des forces de l'ordre avec la population : ouverture au public d'une plate-forme internet de signalement des manquements déontologiques, nouvelles règles déontologiques applicables aux contrôles d'identité et aux palpations de sécurité, évolution en profondeur de la formation des policiers et des gendarmes, ou encore, publication d'une nouvelle version du code de déontologie. Des policiers et des gendarmes mieux respectés et plus proches de la population sont, en effet, plus efficaces. Les caméras-piéton participent de cette logique : professionnaliser et dépassionner les interventions en favorisant la désescalade de la tension, sécuriser les interventions de voie publique des policiers en les objectivant. La caméra constitue en effet un élément de preuve irréfutable sur les conditions d'intervention. Depuis l'automne 2012, une expérimentation de caméras-piéton a été initiée dans plusieurs zones de sécurité prioritaires (ZSP), réservés à des fonctionnaires de police et ds militaires de la gendarmerie travaillant en tenue d'uniforme. A compter de mai 2013, 205 caméras ont ainsi été affectées dans les services de police et unités de gendarmerie compétentes dans les ZSP. S'agissant d'une expérimentation, leur doctrine d'emploi n'est pas encore fixée de manière précise et définitive. Il doit toutefois être souligné que ces caméras n'ont pas à ce stade vocation à filmer des lieux privés. Le cadre juridique est en effet à l'étude pour déterminer les conditions d'emploi des caméras-piéton (enregistrement de toutes les interventions ou des seules situations à risque...consentement des personnes filmées...), la nature des lieux dans lesquels un enregistrement peut être réalisé (lieu public, lieu privé ouvert ou non au public...) et la durée de conservation des données (images et sons). Un projet d'arrêté-cadre relatif au dispositif des caméras est en préparation. Un suivi régulier de l'expérimentation, à partir des retours d'expériences des utilisateurs, est assuré par un comité de pilotage réunissant au niveau central (direction générale de la police nationale) les services techniques et les services opérationnels. Cette instance s'est déjà réunie à quatre reprises. D'ores et déjà, le premier bilan d'utilisation est positif, puisque l'objectif principal est atteint : les caméras « pacifient » les relations entre les utilisateurs et les personnes contrôlées. Par ailleurs, les images et le son sont de très bonne qualité.

7.5 Annexe 5 : Liste des installateurs certifiés

Installateurs certifiés SVDI - Bureau Veritas :

- http://www.interieur.gouv.fr/Videoprotection/La-certification-des-installateurs/La-certification-SVDI-Bureau-Veritas

Installateurs certifiés RI82 AFNOR :
http://www.interieur.gouv.fr/content/download/64819/468741/file/201-09-10-Liste-entreprises-certifiées-afnor.pdf

7.6 Annexe 6 : Formations CNFPT, CNPP, GRETA, AFPA et GPMSE

7.6.1 Répertoire National des Certifications Professionnelles (RNCP) : résumé descriptif de la certification d'opérateur vidéo protection

Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification

Intitulé

Opérateur vidéo protection

Autorité responsable de la certification	Qualité du(es) signataire(s) de la certification
Lycée Jean Moulin - GRETA 34 Ouest	Directeur du Greta

Niveau et/ou domaine d'activité

V (Nomenclature de 1969)

3 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :
344 Sécurite des biens et des personnes, police, surveillance

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

Le titulaire de la certification réalise les activités suivantes :
Prise en compte d'un Centre de Supervision Urbain (CSU).
- Assurer la sécurité d'un CSU.
- Exploiter un système de vidéo protection urbain
- Gérer un système de traitement des alarmes des sites raccordés (Télésurveillance).
- Déclencher et assurer le suivi des interventions selon la typologie des évènements.
- Assurer les aspects techniques et la communication de la gestion des crises ou des grands évènements.
- Rendre compte.

Compétences et capacités techniques:
- connaissance des matériels et des technologies
- application des procédures
- connaissance du cadre légal et règlementaire
- Maîtrise des situations d'alerte

Compétences et capacités comportementales:
- Transmissions; application des consignes
- Capacités de communication
- capacité de concentration, gestion du stress
- travail en équipe mais aussi en autonomie
- Discrétion, respect de la confidentialité et des règles déontologiques

L'opérateur est capable :
- d'appliquer strictement des procédures techniques, transmettre clairement des consignes,
- de maîtriser une situation d'alerte,
- de communiquer clairement,
- d'une attention soutenue pendant un temps relativement long,
- de faire preuve de discrétion.

Secteurs d'activité ou types d'emplois accessibles par le détenteur de ce diplôme, ce titre ou ce certificat

L'opérateur exerce ses fonctions :
- dans les villes ou communautés d'agglomération,
- les PC de sûreté dans les transports publics,
- les salles de vidéo surveillances dans les entreprises recevant du public ou les grands sites industriels.

Opérateur en télésurveillance
Opérateur en vidéo protection
Télévidéosurveilleur

Codes des fiches ROME les plus proches :

K2503 : Sécurité et surveillance privées

Réglementation d'activités :

L'opérateur de télé vidéo-protection doit avoir :
- un casier judiciaire vierge (B2),
- la majorité.

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

1) QCM contrôle écrit des connaissances en matière de :
- Législation, réglementation, déontologie, normes
- Procédures
- Statistiques et caractéristiques de la délinquance
- Techniques et technologies
- Différents services intervenants et leurs prérogatives

2) Entretien évaluation
- La maîtrise de la langue française
- Capacités de transmission des informations
- De demande des consignes
- Relation d'un événement, d'une situation
- Signalement d'une personne, d'un véhicule, d'une scène

3) Mise en situation:
Epreuve d'analyse d'une scène filmée, avec exercice de transmission de l'alerte (téléphone, radio) et relation écrite

La VAE est composée de
- un dossier
- un entretien

Validité des composantes acquises : 5 an(s)

7.6.2 Opérateur de vidéoprotection – CNFPT

MÉTIER

OPÉRATRICE / OPÉRATEUR DE VIDÉOPROTECTION

FAMILLE - PRÉVENTION ET SÉCURITÉ
DOMAINE D'ACTIVITÉS - SÉCURITÉ

Correspondance ROME E/M K2503 Sécurité et surveillance privées

OPÉRATRICE / OPÉRATEUR DE VIDÉOPROTECTION

MÉTIER

Définition	**Contribue à la sécurisation des lieux, des espaces et des bâtiments publics par le biais d'une vidéoprotection. Exploite les images en vue d'informer les partenaires chargés d'intervenir sur les sites**
Facteurs d'évolution	• Développement des politiques de prévention et de sécurité • Accroissement du travail en réseau via les technologies de l'information et de la communication • Développement du secteur privé et fort contexte concurrentiel des activités de surveillance et de gardiennage • Développement technologique de la vidéoprotection • Intensification de la demande sociale en matière de sécurité
Situation fonctionnelle	• Commune, structure intercommunale • Rattaché au responsable du service de police municipale
Conditions d'exercice	• Travail en centre de vidéoprotection en milieu confiné, travail isolé possible • Travail la nuit, en soirée, les week-ends, et les jours fériés • Horaires postés • Risques de fatigue visuelle, physique ou psychologique • Strict respect des procédures et règles de confidentialité • Forte pénibilité limitant la durée d'exercice du métier
Spécialisations / Extensions	• Gestion des alarmes, de la téléphonie et des contrôles d'accès
Autonomie et responsabilités	• Travail contraint, encadré par les textes, règlements et procédures
Relations fonctionnelles	• Relations permanentes avec les services de la collectivité susceptibles d'intervenir sur les sites : police municipale, techniques, maintenance, service de médiation • En fonction des procédures d'information et d'intervention, relations avec les services de la sécurité publique, de la sécurité civile, les sociétés de gardiennage et de surveillance, les entreprises et sous-traitants chargés de la maintenance technique, les sapeurs pompiers
Moyens techniques	• Logiciels d'exploitation des images vidéo et télévisuelles ; système de vidéoprotection, caméras, moyens de radiocommunication, système d'archivage et de destruction des supports vidéo
Cadre statutaire	• Cadre d'emplois : Agents de police municipale (catégorie C, filière Sécurité) • Cadre d'emplois : Adjoints administratifs territoriaux (catégorie C, filière Administrative) • Cadre d'emplois : Adjoints techniques territoriaux (catégorie C, filière Technique)
Conditions d'accès	• Concours externe et interne avec conditions de diplôme et/ou examen d'intégration en fonction du cadre d'emplois, concours troisième voie • Possibilité de recrutement direct pour les cadres d'emplois de catégorie C en fonction du grade (deuxième classe)
Activités techniques	• Observation, analyse et exploitation des images et informations de la vidéoprotection • Participation à la maintenance technique de premier niveau des équipements de vidéoprotection • Contribution au fonctionnement et à l'organisation du centre de supervision urbain (CSU)
Activités spécifiques	• Encadrement d'équipe • Gestion mutualisée de standards

Fiche n° 04/E/34

Centre national de la fonction publique territoriale

ACTIVITÉS/COMPÉTENCES TECHNIQUES

SAVOIR-FAIRE

Observation, analyse et exploitation des images et informations de la vidéoprotection

- Utiliser et maîtriser le système d'exploitation vidéo
- Repérer sur écran des événements significatifs
- Analyser l'information et la relayer vers les services compétents
- Extraire sur réquisition des images enregistrées
- Visionner des images enregistrées dans le cadre légal
- Gérer la traçabilité et l'archivage des images
- Gérer la destruction des images conformément aux règlements et procédures en vigueur
- Déclencher des outils ou différents types d'intervention (alarmes, télésurveillance, astreinte)
- Rédiger des documents de synthèse (main courante, signalements, rapports, etc.)
- Prendre en compte les informations issues des partenaires de la sécurité
- Participer aux coordinations chargées des plans de surveillance et d'intervention

Participation à la maintenance technique de premier niveau des équipements de vidéoprotection

- Vérifier les masquages et champs de vision
- Aider à la définition des cycles automatiques ou des prépositions des caméras
- Signaler les pannes auprès des interlocuteurs compétents
- Aider les techniciens de maintenance dans leur diagnostic

Contribution au fonctionnement et à l'organisation du centre de supervision urbain (CSU)

- Gérer le contrôle d'accès au centre de supervision urbain pour les personnes accréditées
- Alerter les responsables hiérarchiques sur les dysfonctionnements des procédures
- Formuler des propositions d'optimisation des modes opératoires, des procédures et de l'exploitation du cycle des images
- Assurer la prise en compte et la transmission des consignes entre agents et auprès des responsables

SAVOIRS

> SAVOIRS SOCIOPROFESSIONNELS

- Plan communal de sauvegarde
- Procédures et modes opératoires pour la vidéoprotection et la gestion des crises
- Dispositif d'astreinte
- Compétences de la police municipale et nationale et de la gendarmerie dans le cadre des conventions de coordination
- Réglementation de la vidéoprotection, de l'exploitation, de l'archivage et de la destruction des images
- Responsabilité juridique, pénale et sociale liée à la vidéoprotection
- Typologie des publics et connaissances actualisées de la délinquance
- Géographie urbaine et lieux d'implantation des caméras
- Typologie et registre des alarmes
- Charte éthique et déontologique liée à la vidéoprotection
- Logiciels d'exploitation des images télé et vidéo
- Fonctions, composants, connexion des systèmes de vidéo et télésurveillance
- Techniques de maintenance de premier niveau
- Registre de sécurité, règlements internes de la collectivité

> SAVOIRS GÉNÉRAUX

- Procédures hiérarchiques de transmission des consignes et informations
- Organisation des services de la collectivité (police, services techniques)

ACTIVITÉS/COMPÉTENCES TRANSVERSES

ORGANISATION - ENCADREMENT	Code NSF P3	• Encadrement d'équipe
ORGANISATION - ENCADREMENT	Code NSF P3	• Compte-rendu d'activité
SANTÉ ET SÉCURITÉ AU TRAVAIL	Code NSF T3	• Application des règles d'hygiène, de santé et de sécurité au travail

7.6.3 Opérateur de vidéoprotection – CNPP

Secteur privé :

Devenir opérateur privé en vidéosurveillance
VIDEOPRIV

Objectifs

Exercer une activité de vidéosurveillance privée en conformité avec le cadre juridique et réglementaire ainsi que la déontologie propres à la profession.
Assurer la sécurisation préventive et curative de lieux privés dotés d'équipements de vidéosurveillance.
Visionner et exploiter les informations en vue d'informer les partenaires chargés d'intervenir sur les sites.

Profil

Opérateur en station de vidéosurveillance privée (entreprise, grande distribution, etc.) titulaire d'une carte d'agent de prévention et de sécurité.

Contenu

MODULE 1 - Cadre juridique et déontologique - 2 jours

cadre juridique spécifique de la vidéosurveillance (publique - privée / CNIL - Droit du travail),
rôle et obligations légales, déontologiques et professionnelles de l'opérateur de vidéosurveillance privée,
les apports des observations vidéo à la lutte contre la malveillance.

MODULE 2 - Technologie - 1 jour

les caméras, la transmission d'images, l'exploitation avec ou sans stockage, l'association avec d'autres systèmes (contrôle d'accès, détection d'intrusion), la certification, les logiciels d'aide à la surveillance, la maintenance préventive.

MODULE 3 - Méthodologie professionnelle - 1 jour

Méthodes de surveillance et procédures d'exploitation :
- l'usage des moyens vidéo appliqués aux missions de sécurité,
- les méthodes d'observation, de surveillance et d'analyse,
- la prise en compte des niveaux de priorité,
- la gestion de la fatigue et du stress.

MODULE 4 - Application - 1 jour

Exercices pratiques :
- prise de poste : vérifications systématiques de bon fonctionnement,
- mise en place des cadrages de surveillance,
- définition des cadrages de détection et d'identification,
- aide à la gestion de flux et à la surveillance de valeurs,
- levée de doute, demande d'intervention et suivi de l'action,
- recherches dans des enregistrements (« relecture »).

Secteur public :

Devenir opérateur public en vidéoprotection
VIDEOPUB

Objectifs

Assurer la sécurisation préventive et curative des lieux, des espaces et des bâtiments publics dotés d'équipements de vidéosurveillance.
Visionner et exploiter les informations en vue d'informer les partenaires chargés d'intervenir sur les sites

Profil

Opérateur en vidéoprotection affecté en Centre de Supervision Urbain, issu des filières : police municipale, administrative ou technique de la fonction publique territoriale.

Contenu

MODULE 1 - Cadre juridique - 3 jours

Présentation générale de la vidéoprotection.

Cadre juridique et déontologique :
- cadre juridique spécifique de la vidéoprotection,
- obligations légales, déontologiques et professionnelles de l'opérateur de vidéoprotection,
- rôle de l'opérateur de vidéoprotection urbaine,
- les apports des observations vidéo à l'activité de police judiciaire.

MODULE 2 - 1 jour

Méthodes de surveillance et procédures d'exploitation :
- l'usage des moyens vidéo appliqués aux missions de sécurité,
- les méthodes d'observation, de surveillance et d'analyse,
- la prise en compte des niveaux de priorité,
- la gestion de la fatigue et du stress.

MODULE 3 - Application - 1 jour

Exercices pratiques :
- prise de poste : vérifications systématiques de bon fonctionnement,
- mise en place des cadrages de surveillance,
- définition des cadrages de détection et d'identification,
- suivi de foule et ou de trafic routier urbain,
- patrouille vidéo pseudo aléatoire dite « maraude »,
- suivi d'évènement, demande d'intervention policière et suivi de l'action,
- recherches dans des enregistrements.

7.6.4 Opérateur de vidéoprotection – Greta 34 Ouest

académie Montpellier
éducation nationale enseignement supérieur recherche

Greta 34 OUEST
LA FORMATION CONTINUE.

Pezenas
Béziers
Agde

Opérateur de vidéo protection

DOMAINE : Sécurité

PUBLIC CONCERNÉ : Adultes demandeurs d'emploi, salariés d'entreprises de sécurité, salariés de collectivités territoriales.

PRÉREQUIS : Niveau 3ème

Etre capable de :

- Se référer à ses connaissances du cadre légal d'exploitation des images
- D'analyser les étapes d'un comportement délinquant
- De faire intervenir les professionnels par des méthodes d'alerte tout en gardant son calme

CONTENU :
DOMAINES PROFESSIONNELS :

- Cadre légal et réglementaire de la vidéo protection
- Aspects déontologiques et comportementaux
- Environnement quotidien de l'opérateur
- Utilisation de l'outil
- Gestion de crise
-

MÉTHODES PÉDAGOGIQUES : Mise en situation, cours

RECONNAISSANCE EN FIN DE FORMATION : Titre de Niveau V

DURÉE : 70 H de formation
Réduction de parcours possible selon positionnement ou VAE

LIEU DE FORMATION : GRETA 34 OUEST

DATES DE LA FORMATION : à définir

7.6.5 Opérateur en surveillance à distance – AFPA

Opérateur en Surveillance à Distance

Autre(s) appellation(s) : opérateur en videoprotectionAgent de sécurité opérateur-agent d'expolitationagent de sécurité chef de posteopérateur video en magasinagent de sécurité filtrage agent de sécurité qualifié ou confirmé

Domaine :

Rome: K2503
Formacode : 42801
Code AFPA : 11514

Identifiez-vous pour postuler : S'identifier Créer un compte

Objectif | Programme | Admission | Lieux et dates

Le métier

Vous assurez à distance la sécurité des sites de clients (professionnels, particuliers) en traitant les alarmes et ou les imagesprovenant de systèmes de vidéosurveillance ou de vidéoprotection installés sur site dans le respect de la règlementation qui s'applique à ce métier. Vous utilisez les dispositifs et matériels de télésurveillance, vidéosurveillance ou vidéoprotection soit indépendamment soit de façon complémentaire.

En cas d'alarme ou d'anomalie avérée, vous déclenchez les actions définies dans les consignes données par le client, dans le respect de la réglementation en vigueur et des procédures du centre de télésurveillance, de vidéosurveillance ou de videoprotection dans lequel vous exercez votre activité.

Vous participez à la traçabilité de l'activité (main courante informatisée).

En vidéosurveillance ou vidéoprotection, vous exploitez les imagesprovenant des écrans pour assurer une veille continue sur les lieux, espaces ou bâtiments à surveiller.
En télésurveillance, vous assurez la réception, le traitement rapide et efficace des informations reçues et des évènements en fonction des consignes définies.

Pour effectuer ces taches vous vous conformez au code déontologique et aux procédures internes de l'entreprise.

En cas d'évènements, vous écoutez, questionnez et reformulez afin d' établir un constat de la situation et de qualifier la nature et le degré d'urgence. Vous gèrez les déclenchements d'alarme et mobilisez les services d'intervention. Vous prenez des décisions d'urgence adaptées à la situation.

Le diplôme

L'ensemble de ces modules permet d'accéder au titre Opérateur de Surveillance à Distance de niveau IV.

Des qualifications partielles, sous forme de CCP, peuvent être obtenues en suivant 1 ou plusieurs modules. Ces CCP sont les suivants :

CCP - Assurer la surveillance visuelle d'un lieu à l'aide de moyens de vidéosurveillance : Module 1 + Module 2

CCP - Gérer la sécurité des personnes et des biens et réguler l'organisation des interventions au moyen d'un dispositif de télésurveillance : Module 1 + Module 3.

Vous disposez d'un délai de 5 ans, à partir de l'obtention du premier CCP, pour obtenir le titre professionnel.

La carte professionnelle ou l'autorisation préalable seront exigées dans le cadre de la VAE (décret n°2009-137 du 9 février 2009 et ordonnance 202-351 du 12 mars 2012).

Durée

- qualifiant de niveau IV d''une durée modulable de
  4 mois environ (525 heures).
  Les durées mentionnées sur cette fiche sont des durées indicativeset ajustables en fonction des besoins des personnes.
- La durée et le contenu de cette formation sont modulables en fonction des régions et du niveau des participants.

L'organisation de la formation

La formation se compose de 3 modules, complétés par 2 périodes en entreprise.

Période d'intégration : accueil, présentation des objectifs de formation, connaissance de l'environnement professionnel, sensibilisation au développement durable, adaptation du parcours de formation (**1 semaine**).

Module 1. Acquérir le socle de base des aptitudes professionnelles en sécurité privée : les connaissances réglementaires de base **(2 semaines).**

Module 2. Assurer la surveillance visuelle d'un lieu à l'aide de moyens de vidéosurveillance : contrôle des accès par un système de vidéosurveillance ou de vidéo protection - analyse et exploitation des images provenant d'un système de vidéosurveillance ou de vidéo protection pour sécuriser des sites - fonctionnement du système vidéo du centre d'exploitation **(2 semaines)**.

Période en entreprise (**1 semaine**).

Module 3. Gérer la sécurité des personnes et des biens et réguler l'organisation des interventions au moyen d'un dispositif de télésurveillance : traitement des informations - fonctionnement des systèmes de sécurité - intervention en cas d'alarme ou d'anomalie des services compétents - régulation de l'organisation des interventions - fonctionnement et sécurité de la station centrale de télésurveillance - le traitement des communications **(4 semaines)**.

Période en entreprise (**4 semaines**).

Session de validation (**1 semaine**).

Le niveau requis/âge

. Niveau classe de terminale ou première ou équivalent.
. CAP/BEP/Titre professionnel de niveau V dans les métiers de la sécurité (titre A2SP) avec 3 ans d'expérience dans le métier de la sécurité ou de la relation à distance.
. Les candidatures de professionnels de la surveillance, non diplômés, pourront être étudiées et validées si le candidat possède le potentiel et les prérequis.

Une autorisation préalable à l'entrée en formation est indispensable (délivrée par la Commission interrégionale d'agrément et de contrôle (*CIAC*).

Capacité à rédiger un compte rendu informatisé.

L'admission

Dossier de candidature, autorisation préalable (CIAC), évaluations, entretien.

Les aptitudes professionnelles

Exigences physiques : capacité d'attention prolongée, position assise, travail en lieu confiné, bonne résistance nerveuse, travail en soirée, de nuit, les week-ends et jours fériés.
Exigences de moralité : intégrité morale et discrétion, respect des règles et des procédures.
Aptitudes à communiquer : très bonne élocution.
Aptitudes à traiter un grand nombre d'informations visuelles sur écrans.
Aptitude à travailler dans des situations d'urgence.
Ecoute, réactivité, analyse de situations, sens des responsabilités, méthode et rigueur, sens commercial, travail en équipe.

Comment postuler ?

Vous pouvez déposer votre candidature à l'aide d'un formulaire de contact : depuis l'onglet « lieux et dates » si des places sont disponibles.

7.6.6 Technicien en systèmes de surveillance - intrusion et de videoprotection – AFPA

Technicien en systèmes de surveillance - intrusion et de videoprotection (ex-TISI)

J'aime 2

Autre(s) appellation(s) : technicien sécurité-alarme,technicien de maintenance en systèmes d'alarme et de sécurité,technicien de maintenance d'installations automatisées,technicien de maintenance des systèmes d'alarme et de télésurveillance,agent de maintenance en systèmes d'alarme et de sécurité,monteur-installateur d'alarmes,technicien en installations de surveillance intrusion.

Domaine : Electricité, électronique / Prévention, sécurité

Rome: F1602-I1305
Formacode : 42801
Code AFPA : 5228

Identifiez-vous pour postuler : S'identifier Créer un compte

Objectif | Programme | Admission | Lieux et dates | Vidéos

Le métier

Dans le souci de protéger des locaux d'habitation ou les établissements professionnels et de surveiller les comportements humains délictueux (intrusion, vol, agression...), vous installez des systèmes de surveillance, constitués de détecteurs, de caméras, de centrales d'alarme, de sirènes, d'enregistreurs. Vous assurez la mise en service de ces équipements et la formation des utilisateurs. Dans le cadre d'un contrat de service, vous effectuez la maintenance préventive et corrective des systèmes d'alarme installés. Votre lieu de travail se situe soit au sein de l'entreprise pour tout ce qui concerne la gestion et les relations avec le bureau d'études, soit sur le site à surveiller pour ce qui concerne l'installation, l'encadrement des équipes, le suivi technique de chantier et la maintenance des systèmes de surveillance, intrusion et vidéoprotection.

Le diplôme

L'ensemble des modules (5 au total) permet d'accéder au titre professionnel de niveau IV (Bac technique) de technicien en systèmes de surveillance-intrusion et de vidéo protection.

Des qualifications partielles, sous forme de certificats de compétences professionnelles (CCP) peuvent être obtenues en suivant un ou plusieurs modules :

CCP - Installer, mettre en service et dépanner des systèmes de surveillance intrusion et de vidéo protection d'habitations = M1+ M2

CCP - Installer, réaliser le suivi technique de chantier et mettre en service des systèmes professionnels de surveillance intrusion et de vidéo protection = M3 + M4

Vous disposez d'un délai de 5 ans, à partir de l'obtention du premier CCP, pour obtenir le titre professionnel.

Durée

- Formation certifiée de niveau IV d''une durée modulable de 10 mois environ (1 400 heures). Les durées mentionnées sur cette fiche sont des durées indicatives et ajustables en fonction des besoins des personnes.
- La durée et le contenu de cette formation sont modulables en fonction des régions et du niveau des participants.

L'organisation de la formation

La formation se compose de 5 modules, complétés par 2 périodes en entreprise.

Période d'intégration. Accueil, présentation des objectifs de formation, connaissance de l'environnement professionnel, sensibilisation au développement durable, adaptation du parcours de formation **(1 semaine).**

Module 1. Déterminer l'implantation et installer les composants du système de surveillance intrusion et de vidéo protection d'une habitation : réalisation du schéma **d'**implantation et d'installation des composants du système de surveillance intrusion et de vidéo protection d'une habitation **(7 semaines).**

Module 2. Régler, mettre en service et dépanner le système de surveillance intrusion et de vidéo protection d'une habitation : paramétrage du modem-routeur Adsl résidentiel en lien avec le système de surveillance intrusion et devidéo protection d'une habitation - mise enservice du système de surveillance intrusion et de vidéo protection d'une habitation - dépannage et modification d'un système de surveillance intrusion et de vidéo protection d'une habitation **(8 semaines).**

Période en entreprise (3 semaines).

Module 3. Installer, paramétrer, régler et mettre en service un système professionnel de surveillance intrusion et de vidéo protection : installation, paramétrage et réglage des composants du système professionnel de surveillance intrusion - mise en service d'un système professionnel de surveillance intrusion **(8 semaines).**

Module 4. Installer, paramétrer, régler, mettre en service un système professionnel de vidéo protection et de contrôle d'accès : installation, paramétrage, réglage et mise en service d'un système professionnel de vidéo protection ainsi que d'un système professionnel de contrôle d'accès- paramétrage des équipements actifs du réseau informatique en lien avec le système professionnel de surveillance intrusion et de vidéo protection - préparation et suivi technique d'un chantier d'installation du système professionnel de vidéo protection et de contrôle d'accès **(7 semaines).**

Module 5. Assurer la maintenance préventive et corrective de systèmes professionnels de surveillance intrusion et de vidéo protection : planification et réalisation des interventions de dépannage et d'entretien d'un système professionnel de surveillance intrusion et de vidéo protection **(2 semaines).**

Période en entreprise (3 semaines).

Session de validation (1 semaine).

Le niveau requis/âge

Trois profils sont possibles.

1) Niveau classe de 1re technique F2, F3, STI ; ou 2) BEP électronique ; ou 3) expérience professionnelle équivalente au BEP d'une durée de 3 ans dans les métiers de l'électronique.
Extrait n°3 du casier judiciaire.
Permis de conduire B (véhicules légers) indispensable dans l'emploi.

L'admission

Âge minimum : 18 ans.
Dossier de candidature, évaluations, épreuves de connaissances en algèbre-trigonométrie, épreuve de connaissances en électrotechnique, entretien.

Les aptitudes professionnelles

Aptitude aux travaux en hauteur, capacité d'adaptation, sens des responsabilités, rigueur, discrétion, sociabilité, sens commercial.
Les personnes confrontées à des troubles auditifs (fragilité) risquent d'être en difficulté face aux intensités des alarmes.

Comment postuler ?

Vous pouvez déposer votre candidature à l'aide d'un formulaire de contact : depuis l'onglet « lieux et dates » si des places sont disponibles.

7.6.7 Opérateur(trice) spécialisé en traitement d'informations de sécurité à distance (OSTISD) - GPMSE

Cette formation est destinée aux personnels exerçant leur activité dans les stations centrales de télésurveillance, centres de contrôle et de traitement d'informations à distance, centres de sécurité et de supervision.

PRESENTATION

LE CADRE GENERAL Réglementaire / Déontologie	41 Heures
LE METIER Opérateur spécialisé en traitement d'informations de sécurité à distance	115 Heures

TOTAL FORMATION **156 Heures**

EXAMEN Questions écrites - Test QCM Entretien Jury - Mise en situation	2 Heures

1 _ CADRE GENERAL				41 HEURES
MODULE	MODULE	OBJECTIFS PÉDAGOGIQUES généraux	OBJECTIFS PÉDAGOGIQUES spécifiques	DUREE minimale
1-1 Module juridique				**16 heures**
	Environnement juridique de la sécurité privée	Etude Livre VI du Code de la Sécurité intérieure	Maîtriser : – l'explication initiale du livre VI (contexte, logique) ; – l'architecture d'ensemble ; – les conditions d'accès à la profession (moralité et aptitude professionnelle) ; – le principe d'exercice exclusif ; – le principe de neutralité ; – la détention et usage des armes ; – le port des uniformes et insignes ; – les dispositions visant à éviter la confusion avec un service public et sanctions (avec cas concrets) ; – les spécificités des services internes ; – le régime de la carte professionnelle DRACAR et téléc@rtepro.	5 heures
		Connaître les dispositions utiles du code pénal.	Maîtriser les concepts de légitime défense, de faits justificatifs comme l'état de nécessité, d'atteinte à l'intégrité physique et à la liberté d'aller et venir : – les conditions légales de rétention d'une personne avant mise à disposition des forces de police ; – la non-assistance à personne en danger – l'omission d'empêcher un crime ou un délit ; – l'usurpation de fonctions ; – l'atteinte aux systèmes de traitement automatisé ; – l'appropriation frauduleuse ; – le fonctionnement des juridictions pénales.	3 heures
		Application de l'article 73 du code de procédure pénale.	Savoir respecter les conditions d'interpellation de l'article 73 du CPP.	2 heures
		Maîtriser les garanties liées au respect des libertés publiques.	Connaître la législation relative : – au respect de la vie privée ; – au respect du droit de propriété ; – aux juridictions civiles ; – à la CNIL.	2 heures
		Respecter la déontologie professionnelle	Respecter : – le secret professionnel ; – les principes déontologiques. Etre averti sur les marchandages et les sanctions spécifiques associées.	4 heures
1-2 Module stratégique				**25 heures**
	Gestion des premiers secours	Savoir mettre en œuvre les gestes élémentaires de premier secours conformément à la réglementation en vigueur éditée par l'INRS.	Connaître : – le programme national du SST-INRS ou PSC1 ; – la conduite à tenir lors de premiers secours. - savoir alerter et secourir.	14 heures dont 7 heures de mise en pratique

	Gestion des risques et des situations conflictuelles	Savoir analyser les comportements conflictuels	Connaître : – les origines des conflits ; – les différents types de conflits ; – la stimulation et les motivations des conflits ; – les étapes d'un conflit ; – la prévention du conflit.	3 heures
		Savoir résoudre un conflit	Savoir : – traiter une agression verbale ; – gérer les émotions ; – adopter des techniques verbales ; – intervenir par étapes ; – adopter une posture, un regard et une gestuelle adaptés.	2 heures
	Transmission des consignes et informations	Savoir transmettre des consignes	Savoir : – mettre en oeuvre et transmettre des consignes écrites ou orales ; – transmettre des consignes permanentes, particulières ou ponctuelles ; – transmettre des consignes dans le cadre d'une intrusion de malveillance, d'incendie, d'accident.	2 heures
		Réaliser une remontée d'information	Savoir : – faire un compte rendu oral ; – faire un compte rendu écrit ; – faire un rapport.	4 heures

2- CADRE PROFESSIONNEL				**115 heures**
MODULE	MODULE	OBJECTIFS PÉDAGOGIQUES généraux	OBJECTIFS PÉDAGOGIQUES spécifiques	DUREE minimale
2-1 Module de gestion de risque				11 heures
	Gestion des risques	Les risques majeurs	Maîtriser : – les plans de prévention ; – le document unique ; – les plans particuliers d'intervention (PPI, POI, PPRT, etc.) ; – l'organisation de l'intervention ; – la directive SEVESO.	3 heures
		Les risques électriques	Sensibilisation aux risques électriques	4 heures
		Les risques incendie	Savoir : – reconnaître les causes et les effets des incendies ; – utiliser un tableau de signalisation incendie – repérer les agents, les procédés et les matériels ; – organiser une intervention.	4 heures
2-2 La station de Télésurveillance				14 heures
		Connaître - le fonctionnement d'une station centrale de télésurveillance	Savoir - l'architecture, l'informatique - l'organisation	7 Heures

		Connaître - la certification, les critères de qualité	Savoir - la certification de télésurveillance	7 Heures
2-3 Les systèmes de sécurité électroniques				28 heures
	COMPOSITION D'UN SYSTEME DE SECURITE	Connaître - Les technologies utilisées	Savoir - la détection - la signalisation - les organes de commande - la centralisation - la transmission	8 heures
	DOMAINES D'APPLICATION	Connaître - Les missions auxquelles peuvent répondre les stations centrales	Savoir - la télésurveillance - la vidéo surveillance - la vidéo protection - la téléassistance - la détection incendie - le tracking - la protection du travailleur isolé	8 heures
	LES CERTIFICATIONS	Connaître : - Les règles de certification entrant dans la chaîne de sécurité	Savoir - les référentiels existants - les modes d'organisation - les exigences - les procédures	8 heures
	LES RISQUES ELECTRIQUES	Connaître - Les risques en matière électrique	Savoir - manipuler des équipements électriques - l'habilitation électrique	4 heures
2-4 Structure des traitements				28 heures
	GESTION DES EVENEMENTS	Maîtriser - La gestion des évènements	Savoir - analyser et appliquer les procédures	4 heures
	LOGICIELS DE TELESURVEILLANCE	Maîtriser - Les logiciels de télésurveillance	Savoir - la structure des logiciels Métiers	8 heures
	LES ELEMENTS D'UN TRAITEMENT	Maîtriser - Les procédures de traitement de la chaine de sécurité	Savoir - les consignes - la prise en compte d'un évènement / début de traitement - les opérations de levée de doute - l'exploitation et le traitement des images - l'intervention - les forces de l'ordre - les mesures conservatoires - la clôture d'un évènement / fin de traitement	8 heures
	LES PROCESSUS	Connaître - Le traitement d'alarme entraînant des spécificités	Savoir mesurer - l'importance du processus . exemple : l'agression / l'intrusion . exemple : levée de doute audio/ vidéo /autres . exemple : le télé contrôle et télécommande	8 heures
2-5 Le comportement vis-à-vis du client				7 heures
	ACCUEIL TELEPHONIQUE	Maitriser - La relation avec les interlocuteurs	Savoir - la relation client - La relation service d'intervention - la relation avec les secours ou	2 heures

			forces de l'ordre	
	TECHNIQUE COMPORTEMENTALE	Maîtriser - Quel comportement à adopter vis-à-vis des interlocuteurs	Savoir - la gestion du stress - la gestion du temps - l'expression et le formalisme - La gestion de situations de crise - un hold-up - l'agression - l'assistance aux personnes - l'incendie	3 heures
	RENDRE COMPTE	Maîtriser - La rédaction	Savoir - rendre compte - les méthodes	2 heures
2-6 L'opérationnel				27 heures
	PRATIQUE ET EXEMPLES	Maîtriser - Les applications opérationnelles	Savoir - le traitement d'évènements classiques - le traitement d'évènements en état ou situation dégradée - la prise / fin de vacation - la transmission des consignes opérationnelles	27 heures

7.7 Annexe 7 : Liste des principaux organismes

Agence nationale de la sécurité des systèmes d'information (ANSSI)
51, boulevard de La Tour-Maubourg - 75700 Paris 07 SP
Tél. +33 (0)1 71 75 84 05 ou +33 (0)1 71 75 84 06
http://www.ssi.gouv.fr/

Association des utilisateurs interbancaires en télésurveillance (ADITEL)
BP 31012 - 54521 Laxou Cedex
Tél. +33 (0) 820 90 11 44
http://www.aditel-asso.fr/

Association nationale de la vidéoprotection (AN2V)
18, rue Laurent Vibert - 69006 Lyon
Tél. +33 (0)4 78 89 06 37
http://www.an2v-pixel.com/

Association nationale pour la Formation Professionnelle des Adultes (AFPA)
13, place du général de Gaulle – 93108 Montreuil Cedex
Tél. +33 (0)1 48 70 50 00
http://www.afpa.fr/

Centre national de la fonction publique territoriale (CNFPT)
80, rue de Reuilly - CS 41232 - 75578 Paris Cedex 12
Tél. +33 (0)1 55 27 44 00
http://www.cnfpt.fr/

Commission nationale de l'informatique et des libertés (CNIL)
8 rue Vivienne, CS 30223 - 75083 Paris cedex 02
Tél. +33 (0)1 53 73 22 22
http://www.cnil.fr/

Conseil national des activités privées de sécurité (CNAPS)
2-4-6 Bd Poissonnière – CS 70023 – 75009 Paris
Tél. +33 (0)1 48 22 20 40
http://www.cnaps-securite.fr/

Centre national de prévention et de protection (CNPP)
Route de la Chapelle Réanville - CD 64 - CS22265
27950 – Saint Marcel
Tél. +33 (0)2.32.53.64.00
http://www.cnpp.com/

Fédération française des acteurs de formation en sécurité (FFAFOS)
253 rue St Honoré – 75001 Paris -
Tél. +33 (0) 800 823 801
www.unafos.org

Forum Open-IPVideo (Association Loi de 1901 réunissant des professionnels de l'écosystème de la vidéo gestion)
18, rue Irénée Blanc - 75020 Paris
Tél. +33 (0)1 77 02 16 85
http://www.open-ipvideo.org

Groupement Professionnel des Métiers de Sécurité Electronique (GPMSE)
17, rue de l'Amiral Hamelin - 75016 Paris
Tél. +33 (0)1 45 05 71 71
http://www.gpmse.com/

Mission pour le développement de la Vidéoprotection dans l'Agglomération Parisienne (MIVAP)

Syndicat Français des Professionnels (SVDI) (Sécurité voix données images)
5 rue de l'Amiral Hamelin – 75116 Paris
Tél. +33 (0)1 44 05 84 40
http://www.svdi.fr/

Syndicat national des entreprises de sécurité (SNES)
47 rue Aristide Briand - 92300 Levallois Perret
Tél. +33 (0)1 41 34 36 52
http://www.e-snes.org/

Union des entreprises de sécurité privée (USP)
24 rue Firmin Gillot - 75015 Paris
Tél. +33 (0)1 53 58 08 14
http://usp-securite.org/

7.8 Annexe 8 : Liste des membres du groupe de travail

M Philippe ABBAS Chef de produits vidéoprotection DELTA SECURITY SOLUTIONS
M Gilbert AURIC Ingénieur projets STANLEY SECURITY SOLUTIONS (*)
Mme Annick BAILLY Juriste, LA POSTE
M Frédéric BENOIT Directeur de la Police Municipale de Montgeron Police Municipale de Montgeron
Me Alain BENSOUSSAN Président ALAIN BENSOUSSAN AVOCATS
M Jean Charles BENTATA Directeur du CSU de la CAVAM Communauté d'agglomérations de la vallée de Montmorency (CAVAM)
M Ludovic BOURGAIN Gérant R2S TELESURVEILLANCE
Mme Virginie CADIEU Marketing and Communication Director Aasset-security AASSET SECURITY INTERNATIONAL (ASI)
M Olivier CHADEAU Responsable du pôle juridique INTER MUTUELLES TELEASSISTANCE (*)
M Hakim CHALANE Chargé de mission sûreté - Direction de la Cohésion Sociale PARIS HABITAT-OPH
M Philippe COMBEY Directeur IP Sécurité Conseils
M Guy CONAN Directeur 4G TECHNOLOGIES
M Michel COUTANT Coordinateur départemental prévention délinquance CONSEIL GENERAL LOIR ET CHER
M Benoit DAVID Responsable de l'organisation de la sécurité et de la prévention des risques CHAMBRE DE COMMERCE ET D'INDUSTRIE DE PARIS
M M Jonathan DEL PIN Directeur commercial NISCAYAH SAS (*)
Mme Mirelle DESHAYES Chargée coordination I&L GROUPAMA SA NISCAYAH SAS (*)
M Pascal DUFOUR Responsable Sécurité/Assurances Personnes et Biens Banque Populaire Atlantique et Ouest (BPATL) Président de l'Association des utilisateurs interbancaires en télésurveillance (ADITEL)

M Olivier ESTEVENET Juriste B&B HOTELS
M Philippe FRANQUET Président GPMSE INSTALLATION
Mme Julia FULLCHIGNONI Responsable Projets & Développement SECTRANS-CP CONSEILS
M Michel GEORGE Vice-Président GPMSE INSTALLATION
M Nicolas GLEIZAL Directeur SURETIS
M Garry GOLDENBERG Président OPEN IP VIDEO
M Fabien HAUBERT Directeur développement commercial TKH SECURITY SOLUTIONS
M Kévin KHEYARI Enseignant chercheur UNIVERSITE PARIS 2- PANTHEON ASSAS
M Stofa LAKHLEF Directeur Délégué SNC-LAVALIN S.A.S.
Melle Emmanuelle KAWALA Responsable administratif du plan de Vidéoprotection pour Paris
M Dominick LEMULLOIS Directeur Sécurité et Prévention POLICE MUNICIPALE DE MEAUX
Mme Virginie LOGE Sécurité des personnes et biens BNP PARIBAS
M Francisco LOPEZ Directeur de la Police Municipale de Ris Orangis MAIRIE DE RIS ORANGIS
M Pierre-Antoine MAILFAIT Secretaire Général Union des entreprises de sécurité privée (USP)
M Jérémy MARTI Responsable Projets & Développement SECTRANS-CP CONSEILS
Mme Christine MAZIERES Legal Manager MCDONALD'S France
M André MOLINENGO Responsable du Centre de Réception des Alarmes SOCIETE GENERALE
M Guillaume PEGORARI Support technique VINCI FACILITIES
M Dominique POEY Directeur Général des Services Communauté d'Agglomération de la Vallée de Montmorency (CAVAM)

Me Isabelle POTTIER avocat Directeur département Etude et Publications ALAIN BENSOUSSAN AVOCATS
M Philippe POUPEAU Directeur de la Police Municipale d'Evry MAIRIE D'EVRY
M Gilles ROBINE Commandant de Police, Chef de la Mission pour le développement de la Vidéoprotection dans l'Agglomération Parisienne (MIVAP)
M Francis ROLLIN Ingénieur technico commercial GUNNEBO France (*)
M Michel ROUGET SURETE/SF SNCF
M Jean –Edmond ROZOWYKWIAT Directeur technique EXXELL VISION
M Laurent SCETBON Product Marketing Manager ASI Group AASSET SECURITY INTERNATIONAL (ASI)
Mme Elisabeth SELLOS-CARTEL Adjointe au préfet délégué à la sécurité privée MINISTERE DE L'INTERIEUR
M Eugène SIMOES SIRIS-PROTECTION
M Jean-Luc SOLIMENA Directeur régional des opérations STANLEY SECURITY SOLUTIONS
M Jacques TABARD Responsable coordination sécurité réseau France RENAULT
Mme Emmanuelle TANGUY Chef de projet GUNNEBO France (*)
M Claude TARLET Président Union des entreprises de sécurité privée (USP)
Mme Christine TERRACOL Direction de la Sûreté - Département Défense SNCF
M Jean-Michel TEXIER Gérant GROUPE CONVERGENCE
M Régis THEVENET Directeur THEVENET CONSULTANTS
Mme Claire THIEFFRY Référent national PARIS HABITAT-OPH

M Kader TOUAHRI Directeur d'Agence SOCIETE STC - GROUPE SNEF
Mme Stéphanie TUCOULET Secrétaire générale du Syndicat Français des Professionnels SVDI (Sécurité voix données images)
Mme Fabienne VILLARS Cil RENAULT
Me Emmanuel WALLE avocat Directeur département Droit social numérique ALAIN BENSOUSSAN AVOCATS

(*) Membres GPMSE