



**MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER**

*Liberté
Égalité
Fraternité*

Paris, le **20 MARS 2024**

Le ministre de l'Intérieur et des Outre-mer

à

**Monsieur le préfet de police
Mesdames et Messieurs les préfets de département
Monsieur le préfet de police des Bouches-du-Rhône**

Référence	NOR : IOMD2405307J
Date de signature	20 mars 2024
Emetteur	Ministre de l'Intérieur et des Outre-mer
Objet	Mise en conformité du régime de la vidéoprotection avec le droit européen relatif à la protection des données
Commande	Des précisions sont apportées quant à la mise en conformité du régime de la vidéoprotection avec le droit relatif à la protection des données opérée par la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions
Action(s) à réaliser	Veiller à l'application des précisions contenues dans la présente circulaire
Echéance	Effet immédiat
Contact utile	Direction des libertés publiques et des affaires juridiques – Sous-direction des libertés publiques – Bureau du droit des données et des nouvelles technologies Direction des entreprises et partenariats de sécurité et des armes
Nombre de pages et annexes	109 pages dont 5 annexes

Documents annexés :

1. Fiche 1-A : Tableau synthétique relatif aux règles issues de la loi ancienne restées inchangées avec la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 (JOP2024) et aux principales nouveautés apportées par cette loi
2. Fiche 1-B : Evolutions induites par la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions
3. Fiche 2 : Définition des systèmes de vidéoprotection

4. Fiche 3 : Les lieux d'installation des systèmes de vidéoprotection
5. Fiche 4 : Les personnes qui peuvent être autorisées à installer un système de vidéoprotection
6. Fiche 5 : La demande d'autorisation
7. Fiche 6 : Le rôle de la commission départementale de vidéoprotection
8. Fiche 7 : La décision préfectorale
9. Fiche 8 : Les contrôles et sanctions
10. Annexe 1 : Modèle d'AIPD « cadre » pour les autorités publiques
11. Annexe 2 : Modèle d'AIPD pour les autorités privées
12. Annexe 3 : Formulaire Cerfa n° 13810*03 - Déclaration simplifiée - Engagement de conformité
13. Annexe 4 : Formulaire CERFA n°13806*04 - Demande d'autorisation d'un système de vidéoprotection
14. Annexe 5 : Notice d'information relative au formulaire CERFA n° 13806*03 - Demande d'autorisation d'un système de vidéoprotection

Depuis la création de son cadre juridique par la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, la vidéoprotection s'est largement développée comme un outil d'amélioration de la sécurité de nos concitoyens et apparaît désormais pleinement acceptée.

La vidéoprotection est un outil efficace, qui bénéficie par conséquent d'un effort budgétaire important du fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR) dont les crédits destinés à la vidéoprotection seront triplés au cours des cinq années à venir et viendront cofinancer les projets portés par les collectivités territoriales, notamment des audits des éventuelles failles de sécurité présentes dans les caméras déjà installées, comme l'indique le rapport annexé à la LOPMI promulguée le 24 janvier 2023.

A cet effort financier devait correspondre une mise à niveau juridique.

Il était en effet impératif de mettre en conformité le cadre légal de la vidéoprotection « fixe » avec le nouveau cadre juridique relatif à la protection des données à caractère personnel entré en vigueur en 2018, issu des règles du règlement général sur la protection des données (RGPD) et de la directive dite « *police-justice* », les dispositions relatives aux caméras mobiles (caméras-piétons, aéroportées, embarquées) ayant, quant à elles, déjà été récemment mises en conformité. Alors que la vidéoprotection était considérée par une jurisprudence européenne constante¹ comme un traitement de données à caractère personnel, la loi précitée de 1995 prévoyait plusieurs règles dérogatoires en matière de droit des personnes filmées et de droit de contrôle de la Commission nationale de l'informatique et des libertés (CNIL).

L'article 9 de la loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2023 et portant diverses autres dispositions*, complétée par le décret n° 2023-1102 du 27 novembre 2023², ont procédé à cette actualisation indispensable, en renforçant les obligations qui pèsent sur les responsables de systèmes de vidéoprotection et le contenu du dossier de demande d'autorisation, et en rendant pleinement effectifs les droits des personnes et les pouvoirs de contrôle et de sanction de la CNIL. Cette actualisation était en outre rendue nécessaire par la prochaine expérimentation de la vidéoprotection « *intelligente* », que la même loi précitée a autorisée, pour une mise en œuvre à compter des marchés de Noël 2023 et jusqu'au 31 mars 2025³.

Au terme de cette réforme, les préfets conservent un rôle central en matière de vidéoprotection :

- Vous demeurez décisionnaires pour **autoriser ou rejeter les demandes d'installation de systèmes de vidéoprotection**. Le dossier de demande soumis à l'instruction de vos services sera enrichi, en particulier du fait de la nécessité pour les responsables de traitement dans certains cas d'y adjoindre une analyse d'impact relative à la protection des données (AIPD) et un engagement de conformité à la CNIL (cf. fiche n° 1-B) ;
- vous pouvez faire procéder par les services de police ou de gendarmerie à des **contrôles de vérification** des prescriptions émises dans les autorisations préfectorales ;
- vos services continuent à assurer **le secrétariat de la commission départementale de vidéoprotection**, cette dernière pouvant diligenter des contrôles de sa propre

¹ CJUE, 11 décembre 2014, C-212/13.

² Décret n° 2023-1102 du 27 novembre 2023 portant application des articles L. 251-1 et suivants du code de la sécurité intérieure et relatif à la mise en œuvre des traitements de données à caractère personnel provenant de systèmes de vidéoprotection et des caméras installées sur des aéronefs.

³ Article 10 de la loi n° 2023-380 du 19 mai 2023 et décret n° 2023-828 du 30 août 2023.

initiative ou sur saisine, et vous proposer le cas échéant la suspension ou la suppression d'un système lorsqu'elle constate qu'il n'est pas autorisé ou qu'il en est fait un usage anormal ou non conforme à son autorisation ;

- lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, vous conservez la faculté de **délivrer aux autorités publiques compétentes ou aux personnes morales concernées une autorisation provisoire** d'installation d'un système de vidéoprotection sans avis préalable de la commission départementale de vidéoprotection ;
- vous pouvez enfin **demander à une commune la mise en œuvre de systèmes de vidéoprotection** aux fins de prévention d'actes de terrorisme ou de protection des abords des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ou de protection des intérêts fondamentaux de la Nation.

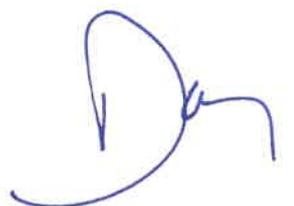
Dans la mesure où la loi précitée laisse inchangé le régime d'autorisation des systèmes de vidéoprotection, vous n'avez pas besoin de prendre de nouvelles autorisations pour les systèmes déjà déployés et autorisés dans votre département.

Les fiches annexées à la présente circulaire, qui abroge et remplace les circulaires des 12 mars 2009 et 14 septembre 2011, résument les évolutions induites par la loi du 19 mai 2023 précitée et précisent les modalités de mise en œuvre des systèmes de vidéoprotection.

Elles sont également accessibles sur l'intranet de la direction des libertés publiques et des affaires juridiques (DLPAJ), qui, régulièrement actualisé, doit constituer votre support d'information juridique privilégié (<https://intranet.dlpaj.minint.fr/>).

Concernant en particulier les systèmes de vidéoprotection des collectivités territoriales, vous pouvez vous référer à l'instruction du Gouvernement du 4 mars 2022 relative à la mise en œuvre des dispositions de la loi du 25 mai 2021 et portant sur l'acquisition, l'installation et l'entretien de dispositifs de vidéoprotection par les collectivités territoriales et leurs groupements ainsi que sur l'habilitation du personnel territorial procédant au visionnage, publiée au bulletin officiel du ministère de l'Intérieur du 11 mars 2022.

Vous veillerez à la bonne application de ces précisions par l'ensemble des services sous votre autorité et vous voudrez bien me tenir informé, sous le présent timbre, de toute difficulté d'application de la présente circulaire. Je compte sur vous pour exploiter le potentiel considérable de la vidéoprotection en veillant à la stricte application du droit qui l'encadre.



Gérald DARMANIN

Fiche n° 1-A : Tableau synthétique relatif aux règles issues de la loi ancienne restées inchangées avec la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 (JOP2024) et aux principales nouveautés apportées par cette loi nouvelle

	Règles juridiques actuelles restées inchangées	Principales nouveautés apportées par la nouvelle réglementation
Autorisation d'un système de vidéoprotection		
Instruction de la demande d'autorisation du système de vidéoprotection (Cf. fiches n° 5 et 7)	Les personnes autorisées à installer un système de vidéoprotection doivent constituer un dossier de demande d'autorisation comportant une liste de pièces (cf. fiche n° 5)	<p>Le dossier de demande ne contient plus:</p> <ul style="list-style-type: none"> - les consignes générales données aux personnels d'exploitation du système de vidéoprotection pour le fonctionnement de celui-ci et le traitement des images ; <p>Dans certaines circonstances, le dossier de demande comporte deux nouvelles pièces :</p> <ul style="list-style-type: none"> - une analyse d'impact relative à la protection des données (AIPD), pouvant remplacer certaines pièces du dossier ; - un engagement de conformité destiné à la CNIL. <p>Dans le cadre de sa mission consultative, la commission départementale de vidéoprotection (CDV) devra également examiner ces deux nouvelles pièces (cf. fiche n° 6 sur le rôle des CDV).</p>
Décision d'autorisation préfectorale (cf. fiche n° 7)	L'autorisation préfectorale prévoit toutes les précautions utiles (délai de conservation des images, mesures de sécurité, personnes pouvant accéder au visionnage des images et personnes pouvant en être destinataires, etc.) pour être conforme au cadre juridique applicable à la vidéoprotection.	La liste des personnes pouvant accéder au visionnage des images et des personnes pouvant en être destinataires a été clarifiée et précisée.
Modification des demandes d'autorisation d'un système de vidéoprotection (cf. fiche n° 7)	Lorsque le responsable de système souhaite apporter des modifications à un système, le préfet doit évaluer la nécessité de délivrer une nouvelle autorisation.	Pas de changement
Renouvellement des demandes d'autorisation d'un système de vidéoprotection (cf. fiche n° 7)	Lorsque l'autorisation arrive à expiration, le responsable de système doit demander le renouvellement de sa demande en déposant un nouveau dossier complet, qui devra être instruit par le préfet.	Pas de changement
Procédures particulières d'autorisation		
Prescription préfectorale de mise en œuvre d'un système de vidéoprotection (cf. fiche n° 7)	Le préfet peut prescrire la mise en œuvre de systèmes de vidéoprotection aux fins de prévention d'actes de terrorisme ou en cas d'urgence et d'exposition particulière à un risque d'actes de terrorisme ou lorsque le préfet a été informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers.	Pas de changement

<p>Autorisation provisoire de mise en œuvre d'un système de vidéoprotection (cf. fiche n° 7)</p>	<p>Le préfet peut délivrer une autorisation provisoire d'installation d'un système de vidéoprotection, lorsque l'urgence et l'exposition particulière à un risque d'acte de terrorisme le requièrent ou lorsqu'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers.</p>	<p>Pas de changement</p>
<p>Demande préfectorale de mise en œuvre d'un système de vidéoprotection (cf. fiche n° 7)</p>	<p>Le préfet peut demander à une commune la mise en œuvre de systèmes de vidéoprotection, aux fins de prévention d'actes de terrorisme, de protection des abords de certains établissements, installations ou ouvrages ou de protection des intérêts fondamentaux de la Nation.</p>	<p>Pas de changement</p>
<p>Garanties et droits accordés aux personnes filmées par un système de vidéoprotection</p>		
<p>Droits des personnes concernées (cf. fiche n° 1-B)</p>	<p>Le préfet doit vérifier les modalités de l'information du public et celles de leur droit d'accès. Les personnes concernées sont informées de la mise en œuvre d'un système de vidéoprotection, par voie d'affiches ou de panneaux sur les lieux d'installation des caméras, comportant un pictogramme représentant une caméra et des informations permettant d'identifier le responsable du système.</p>	<p>La liste des informations à mettre à la disposition du public a été substantiellement enrichie. Il doit désormais être fait, par exemple, mention de la durée de conservation des données, des destinataires ou catégories de destinataires des données ou encore de nouveaux droits (il a été ajouté, en complément du droit d'accès, un droit de rectification, d'effacement et à la limitation des données).</p> <p>Cette liste de mentions d'information diffère en fonction du régime juridique applicable au système de vidéoprotection. (cf. fiche n° 1-B).</p>
<p>Contrôles et sanctions</p>		
<p>Contrôles (Cf. fiche n° 8)</p>	<p>La CDV peut exercer des contrôles visant à vérifier la conformité du système de vidéoprotection à son autorisation et proposer au préfet des sanctions en cas de non-respect des conditions d'autorisation du système.</p> <p>Le préfet peut faire procéder, par les services de police ou de gendarmerie, à des contrôles de vérification des prescriptions émises dans les autorisations préfectorales, sur l'existence de systèmes non autorisés et sur la conformité du système aux normes techniques.</p>	<p>Pas de changement</p>
<p>Sanctions (Cf. fiche n° 8)</p>	<p>A l'issue du contrôle qu'elle peut exercer sur les systèmes de vidéoprotection, la CDV peut proposer au préfet la suspension de l'autorisation d'installation ou le retrait de l'autorisation d'installation.</p> <p>Le préfet peut également demander la fermeture administrative de l'établissement ou enjoindre de démonter le système de vidéoprotection.</p> <p>La mise en œuvre d'un système de vidéoprotection sans autorisation préalable constitue un délit.</p>	<p>Pas de changement</p>

Fiche n° 1-B : présentation des modifications du régime juridique de la vidéoprotection par l'article 9 de la loi n° 2023-380 du 19 mai 2023 relative aux Jeux olympiques et Paralympiques de 2024 et portant diverses autres dispositions

I. L'application des règles relatives à la protection des données aux systèmes de vidéoprotection

Alors que le code de la sécurité intérieure ne prévoyait l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « informatique et libertés ») qu'aux enregistrements de vidéoprotection utilisés dans des fichiers structurés selon des critères permettant d'identifier les personnes, l'article 9 de la loi du 19 mai 2023 soumet l'ensemble de la vidéoprotection aux dispositions de cette loi.

Dès lors, les responsables des systèmes de vidéoprotection doivent se mettre en conformité avec la loi « informatique et libertés » en se faisant accompagner, le cas échéant, par leur délégué à la protection des données.

Le rôle des préfets est distinct de celui des responsables des systèmes de vidéoprotection : il consiste, lors de l'autorisation des systèmes, à veiller à l'effectivité de cette mise en conformité, en contrôlant en particulier la production par les responsables de systèmes des pièces nécessaires.

A. La détermination du régime juridique applicable

Les traitements de données à caractère personnel issus des systèmes de vidéoprotection peuvent, selon leur finalité et la qualité du responsable du système, relever de différents régimes de protection des données à caractère personnel prévus par la réglementation européenne et par la loi « informatique et libertés ».

La détermination du régime juridique adéquat est essentielle, dans la mesure où le champ dont relève le traitement entraîne des conséquences notables à plusieurs niveaux, notamment quant aux droits des personnes concernées et aux obligations imposées aux responsables de traitement.

Il appartient aux responsables de système de vidéoprotection de déterminer le régime applicable à leur système. Les développements ci-dessous présentent les différents régimes susceptibles de s'appliquer.

1. Le titre IV de la loi « informatique et libertés » : les systèmes de vidéoprotection qui intéressent la sûreté de l'Etat et la défense

Ce régime juridique est applicable aux traitements qui sont mis en œuvre pour le compte de l'Etat et qui intéressent la sûreté de l'Etat et la défense.

Concrètement, ce régime juridique ne concerne que les systèmes de vidéoprotection mis en œuvre par le ministère des armées pour assurer la sauvegarde des installations utiles à la défense nationale (le 2° de l'article L. 251-2 du code de la sécurité intérieure).

2. Le titre III de la loi « informatique et libertés » (issu de la directive dite « police-justice ») : les systèmes de vidéoprotection mis en œuvre à des fins « police-justice »

Les systèmes de vidéoprotection peuvent relever de ce régime lorsqu'ils remplissent deux critères cumulatifs prévus à l'article 87 de la loi « informatique et libertés » :

1. Ils poursuivent des **fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces**. Une analyse au cas par cas, au regard des circonstances particulières, doit être menée par le responsable du système pour déterminer si ce dernier poursuit une de ces finalités.
2. Ils sont mis en œuvre par une **autorité compétente pour ces fins** : par « autorité compétente », il faut entendre toute autorité publique ou tout autre organisme ou entité à qui a été confié, aux fins précitées, l'exercice de l'autorité publique et des prérogatives de puissance publique. Peu de services sont des autorités compétentes au sens de la loi « informatique et libertés ». C'est le cas par exemple des services de la police nationale et de la gendarmerie nationale ou encore d'un maire. A l'inverse, ne sont par exemple pas des « autorités compétentes » le responsable d'un établissement scolaire ou hospitalier, le responsable d'un service d'incendie ou de secours ou un commerçant.

Concrètement, ce régime juridique s'applique essentiellement aux systèmes de vidéoprotection mis en œuvre par les services de la police nationale et de la gendarmerie nationale et par les communes.

3. Le RGPD et le titre II de la loi « informatique et libertés » : les autres systèmes de vidéoprotection

Les systèmes de vidéoprotection peuvent relever de ce régime juridique lorsqu'ils n'entrent ni dans le champ du titre III, ni dans celui du titre IV de la loi « informatique et libertés », soit parce que leur finalité n'intéresse pas la sûreté de l'Etat ou la défense ou la « police-justice », soit parce que le responsable de ces traitements n'est pas une autorité compétente au sens de cette loi.

Sauf si elles se sont vues confier l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces (exemple : les fédérations sportives agréées aux fins de sécurisation des manifestations sportives), les systèmes de vidéoprotection mis en œuvre par des personnes privées relèvent par principe du RGPD et du titre II de la loi « informatique et libertés ».

Concrètement, ce régime juridique s'applique « par défaut » lorsque les deux régimes spécifiques prévus par le titre IV et le titre III de la loi « informatique et libertés » ne s'appliquent pas. Il concerne donc la majeure partie des systèmes de vidéoprotection mis en œuvre.

4. L'application d'un régime mixte en cas de finalités multiples

La mise en œuvre de systèmes de vidéoprotection pour plusieurs finalités peut conduire à l'application simultanée de plusieurs régimes de protection des données (titre IV, titre III et/ou titre II de la loi « informatique et libertés »).

Dans ce cas, le responsable du système de vidéoprotection devra distinguer les régimes applicables en fonction des finalités de son système.

Personnes	Finalités	Titre pouvant être applicable
	La protection des bâtiments et installations publiques et de leurs abords	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne ⁴ : Titre II
	La sauvegarde des installations utiles à la défense nationale	Titre IV
	La régulation des flux de transport	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La constatation des infractions aux règles de la circulation	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La prévention d'actes de terrorisme	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
Autorités publiques	La prévention des risques naturels ou technologiques	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	Le secours aux personnes et la défense contre l'incendie	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La sécurité des installations accueillant du public dans les parcs d'attraction	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	Sécurité des personnes et des biens dans les lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol	Autorité compétente au sens de la directive : Titre III Autre autorité ou personne : Titre II
	Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
Personnes morales de droit privé, y compris les commerçants	Protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme	Titre II
	Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol	Titre II
	Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme	Titre II
Commerçants uniquement	Protection des abords immédiats de leurs bâtiments et installations dans les lieux particulièrement exposés à des risques d'agression ou de vol	Titre II

⁴ Signifie que le responsable du système n'est pas une autorité compétente aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces

B. La rédaction d'une analyse d'impact relative à la protection des données (AIPD)

En application du RGPD et de la loi « informatique et libertés », la mise en œuvre de systèmes de vidéoprotection peut être subordonnée à la réalisation d'une analyse d'impact relative à la protection des données (AIPD)⁵.

L'AIPD permet de démontrer la conformité du système de vidéoprotection envisagé au regard de la réglementation applicable en matière de protection des données à caractère personnel. Elle vise à présenter le traitement (sa nature, sa portée, son contexte, ses finalités et ses enjeux), à en évaluer la nécessité ainsi que la proportionnalité et à aider le responsable du traitement à gérer les risques pouvant affecter les droits et libertés des personnes physiques concernées en les évaluant et en déterminant les mesures nécessaires pour y faire face.

Le cas échéant, il appartient à la personne ou au service qui demande l'autorisation d'installer un système de vidéoprotection d'élaborer cette AIPD. Si une AIPD est réalisée, elle a vocation à remplacer certaines pièces du dossier de demande d'autorisation (cf. fiche n°5).

1. Situations dans lesquelles la rédaction d'une AIPD est obligatoire

La rédaction d'une AIPD est obligatoire dans l'hypothèse où le système de vidéoprotection est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Cette obligation n'est pas applicable en matière de défense nationale.

Dans cette optique, la CNIL a établi une liste de **neuf critères** permettant de déterminer si un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes :

- Evaluation ou notation (« *scoring* ») (y compris les activités de profilage et de prédiction) ;
- Prise de décision automatisée avec effet juridique ou effet similaire significatif ;
- Surveillance systématique ;
- Collecte de données sensibles ou données à caractère hautement personnel ;
- Données traitées à grande échelle ;
- Croisement ou combinaison d'ensembles de données ;
- Données concernant des personnes vulnérables (personnes âgées, enfants, etc.) ;
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD. D'une manière générale, plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD. Néanmoins, dans certains cas, le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD.

⁵ Pour plus d'informations sur l'AIPD, voir le site de la CNIL : <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>

Au regard des éléments caractéristiques des systèmes de vidéoprotection, les critères de « la surveillance systématique » et de la « collecte de données personnelles à large échelle » sont susceptibles d'être remplis.

Cette AIPD devra être jointe à la demande d'autorisation du système.

2. Modèles d'AIPD

Afin de faciliter le travail d'analyse, il est proposé en annexe de cette circulaire deux modèles d'AIPD qui pourront être communiqués au demandeur :

- Pour les autorités publiques : il s'agit de l'AIPD « cadre » présentée à la CNIL lors de l'élaboration du décret n° 2023-1102 du 27 novembre 2023 précité. Elle a vocation à constituer le socle de référence des garanties minimales à mettre en œuvre destinées à préserver les droits et libertés et à assurer le fonctionnement du système en conformité avec les exigences de la loi « informatique et libertés ». Si cette trame est utilisée par le responsable du système de vidéoprotection, ce dernier doit la compléter par les éléments nécessités par les circonstances locales (champs surlignés en jaune).
- Pour les personnes privées : il s'agit d'une proposition de modèle pré-rempli avec les éléments communs à l'ensemble des systèmes de vidéoprotection.

C. La rédaction d'un engagement de conformité

Lorsqu'un traitement répond à une même finalité, porte sur des catégories de données identiques et a les mêmes destinataires ou catégories de destinataires et qu'il fait ainsi l'objet d'un acte réglementaire unique au sens du IV de l'article 31 de la loi « informatique et libertés », chaque responsable de traitement adresse à la CNIL un engagement de conformité de celui-ci à la description figurant dans cet acte.

L'article R. 253-7 du code de la sécurité intérieure subordonne ainsi la mise en œuvre des systèmes de vidéoprotection à l'envoi préalable de cet engagement de conformité et prévoit que certains responsables de systèmes de vidéoprotection doivent adresser à la CNIL un engagement de conformité.

L'article R. 253-7 du code de la sécurité intérieure subordonne la mise en œuvre d'un système de vidéoprotection par une autorité publique à l'envoi préalable à la CNIL d'un engagement de conformité aux dispositions réglementaires.

Cette formalité ne s'impose qu'aux autorités publiques, donc notamment aux services de l'Etat centraux et déconcentrés ainsi qu'aux collectivités territoriales.

L'engagement de conformité est joint au dossier de demande d'autorisation auprès du préfet mais ne doit être envoyé à la CNIL qu'après autorisation du système de vidéoprotection par ce dernier.

Le formulaire d'engagement de conformité (Cerfa n° 13810*03) figure en annexe. À la rubrique 2, la case « Acte réglementaire unique » devra être cochée et complétée par le « N° de référence », en l'occurrence RU-74.

L'engagement de conformité peut également être réalisé en ligne, sur le site de la CNIL à la rubrique « Effectuer une déclaration de conformité » : <https://www.cnil.fr/fr/declarer-un-fichier>

II. Les droits des personnes concernées par un système de vidéoprotection

A. L'information des personnes concernées

Par principe, le public doit être informé par la personne ou le service responsable de la mise en œuvre d'un système de vidéoprotection.

Les informations à mettre à la disposition du public diffèrent en fonction du régime applicable au système de vidéoprotection (cf. I). Il s'agit des informations mentionnées :

- Dans la section 2 du chapitre III du RGPD s'agissant des systèmes relevant de ce règlement et du titre II de la loi « informatique et libertés » ;
- A l'article 104 de la loi « informatique et libertés » s'agissant des systèmes relevant du titre III de cette loi
- A l'article 116 de la loi « informatique et libertés » s'agissant des systèmes relevant du titre IV de cette loi

Le tableau ci-après détaille les informations devant être obligatoirement fournies aux personnes concernées par le traitement en fonction du régime juridique applicable au traitement.

RGPD et titre II de la loi « informatique et libertés » Article 13 du RGPD	Titre III de la loi « informatique et libertés » Article 104 de la loi « informatique et libertés »	Titre IV de la loi « informatique et libertés » Article 116 de la loi « informatique et libertés »
L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement	L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement	L'identité du responsable du traitement et, le cas échéant, de celle de son représentant
Le cas échéant, les coordonnées du délégué à la protection des données	Le cas échéant, les coordonnées du délégué à la protection des données	
Les finalités du traitement auquel sont destinées les données à caractère personnel	Les finalités poursuivies par le traitement auquel les données sont destinées	La finalité poursuivie par le traitement auquel les données sont destinées
La base juridique du traitement, soit les articles L. 251-2 et suivants du code de la sécurité intérieure	La base juridique du traitement, soit les articles L. 251-2 et suivants du code de la sécurité intérieure	
Le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel	Le cas échéant, les catégories de destinataires des données à caractère personnel, y compris ceux établis dans les Etats n'appartenant pas à l'Union européenne ou au sein d'organisations internationales	Les destinataires ou catégories de destinataires des données
Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne ou d'une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne, ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition		Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne
La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée	La durée de conservation des données à caractère personnel ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée	La durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.
Lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f) du RGPD, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers		
L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée.	L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée	Les droits que la personne concernée tient des dispositions des articles 117 à 120 de la loi « informatique et libertés »
Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés	Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission	

D'autres informations additionnelles peuvent être adressées aux personnes concernées par le responsable du système, conformément au II de l'article 104 de la loi « informatique et libertés ».

En application de l'article R. 253-6 du code de la sécurité intérieure, cette information doit être délivrée par voie d'affiches ou de panneaux sur les lieux d'installation des caméras, comportant un pictogramme représentant une caméra.

Par exception, un double niveau d'information peut être délivré si le responsable le souhaite. Dans ce cas :

- les affiches ou panneaux doivent mentionner au minimum l'identité du responsable du système, les finalités poursuivies par le traitement et les droits des personnes concernées ;
- les autres informations exigées par le RGPD ou la loi « informatique et libertés » peuvent être communiquées par tout autre moyen, par exemple par le biais d'un renvoi vers un site internet.

En tout état de cause, les modalités d'information (format, nombre et localisation des affiches ou panneaux) doivent être adaptées aux circonstances dans lesquelles elles sont déployées, notamment à la situation des lieux et établissements.

Les modalités d'information font partie du dossier de demande. **Le préfet doit donc, à ce titre, les contrôler.**

B. Les droits d'accès, de rectification, à la limitation, d'effacement des données et d'opposition

Dans leur demande d'autorisation, les responsables de systèmes doivent détailler les modalités d'information du public, et, à ce titre, la façon dont les personnes pourront exercer leurs droits auprès d'eux.

Il appartient au préfet de vérifier que l'information des personnes précise l'ensemble de leurs droits prévus par le RGPD et la loi. La personne ou le service à contacter pour exercer leur droit d'accès ainsi que ses coordonnées doivent être précisés dans le dossier de demande d'autorisation.

Avant l'entrée en vigueur de la loi du 19 mai 2023, le code de la sécurité intérieure ne conférait aux personnes que le droit d'obtenir un accès aux enregistrements qui les concernaient.

Ce droit est maintenu et permet aux personnes concernées de demander au responsable de traitement si des données les concernant ont ou n'ont pas été traitées et d'en obtenir l'accès. Cet accès, demandé par écrit ou sur place, se matérialise par un visionnage des images qui concernent la personne ou par la fourniture d'une copie de ces images, après y avoir appliqué un système de « floutage » permettant de protéger les droits des tiers.

L'article R. 253-6 du code de la sécurité intérieure prévoit que le responsable de système de vidéoprotection peut, pour garantir la sécurité nationale ou la protection contre les menaces pour la sécurité publique ou la prévention de telles menaces, restreindre le droit d'accès des personnes.

La mise en conformité du régime de la vidéoprotection avec le droit sur la protection des données entraîne en principe l'ouverture de nouveaux droits aux personnes⁶ :

- Droit à l'effacement : les personnes concernées peuvent demander au responsable de traitement d'effacer les données à caractère personnel les concernant dans les meilleurs délais. Lorsque le système de vidéoprotection relève du RGPD et du titre II de la loi « informatique et libertés » et qu'il est nécessaire pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit à l'effacement ne s'applique pas ;
- Droit à la limitation du traitement : les personnes concernées peuvent demander au responsable de traitement d'arrêter, temporairement, d'utiliser certaines données.

L'article R. 253-6 du code de la sécurité intérieure prévoit que le droit d'opposition n'est pas applicable au traitement : les personnes concernées ne peuvent pas s'opposer au traitement de leurs données à caractère personnel.

Pour exercer leurs droits, les personnes concernées s'adressent directement au responsable du système de vidéoprotection.

III. La mise en conformité des systèmes de vidéoprotection existants

Dans la mesure où le décret n° 2023-1102 du 27 novembre 2023 précité met en conformité le cadre juridique des systèmes de vidéoprotection avec les règles relatives à la protection des données, de nouvelles obligations s'imposent aux systèmes déjà autorisés.

D'une part, si une AIPD est obligatoire (cf. partie I. B.), le responsable du système devra la rédiger.

De plus, pour les systèmes mis en œuvre par les autorités publiques, les responsables de traitement devront envoyer un engagement de conformité à la CNIL.

Enfin, le contenu de l'information faite à destination des personnes susceptibles d'être filmées doit être adapté aux nouvelles exigences juridiques.

Il n'est néanmoins pas nécessaire de prendre de nouvelles autorisations pour les systèmes déjà déployés et autorisés.

⁶ Le droit de rectification s'applique en principe à tout traitement. Les personnes concernées peuvent donc normalement demander au responsable d'un traitement que les données à caractère personnel les concernant, qui sont inexacts, soient rectifiées dans les meilleurs délais ou soient complétées. La portée de sa mise en œuvre pour des enregistrements vidéo est *a priori* limitée.

Fiche n°2 : Définition des systèmes de vidéoprotection

Les systèmes de vidéoprotection se définissent par la réunion de différents critères tenant à la technique utilisée, aux lieux filmés et aux finalités poursuivies, ainsi qu'à la personne qui les met en œuvre. Cette définition n'a pas été modifiée par la loi du 19 mai 2023 et reste inchangée.

Techniquement, ces systèmes consistent en l'usage d'au moins une caméra et d'un moniteur, c'est-à-dire un écran permettant la visualisation des images.

La ou les caméras sont installées sur la voie publique ou dans les lieux ou établissements ouverts au public qu'elles permettent de filmer.

Les systèmes de vidéoprotection sont à distinguer des systèmes de vidéosurveillance qui, depuis la loi du 14 mars 2011, désignent des systèmes installés dans les lieux privés ou les lieux professionnels non ouverts au public.

La captation d'images issues de systèmes de vidéoprotection, qu'elle donne lieu à un visionnage des images filmées en temps réel sans conservation ou à un enregistrement, constitue un traitement de données à caractère personnel, au sens du RGPD et de la loi « informatique et libertés ». En effet, les images sur lesquelles apparaissent des personnes qui peuvent être identifiées livrent des informations relatives notamment à leur présence à un endroit et un moment déterminés.

Les systèmes de vidéoprotection ne peuvent pas capter de sons⁷.

A l'inverse, certains dispositifs ne constituent pas des systèmes de vidéoprotection. A titre d'exemple, les dispositifs de contrôle automatisé des données signalétiques des véhicules, plus communément appelés lecture automatisée de plaques d'immatriculation (LAPI), ne constituent pas des systèmes de vidéoprotection.

Il en va de même pour les dispositifs de pièges photographiques ou encore des caméras mobiles (caméras individuelles, caméras installées sur des aéronefs ou caméras embarquées) autorisées dans les cas définis par le titre IV du livre II de la partie législative du code de la sécurité intérieure.

⁷ Article R. 253-1 du code de la sécurité intérieure : « Peuvent être enregistrées dans les traitements mentionnés à l'article R. 251-1, les données à caractère personnel et informations suivantes : « 1° Les images, à l'exclusion des sons, captées par les systèmes de vidéoprotection ; [...] ».

Fiche n°3 : Les lieux d'installation des systèmes de vidéoprotection

Le régime d'autorisation préfectorale de l'article L. 252-1 du code de la sécurité intérieure (auquel renvoie l'article L. 223-1 du même code) ne s'applique qu'aux systèmes installés sur la voie publique ainsi que dans les lieux et établissements ouverts au public. Cette définition n'a pas été modifiée par la loi du 19 mai 2023 et reste inchangée.

I. La voie publique

Un système de vidéoprotection installé sur la voie publique ne saurait visualiser les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées. Si un tel système filme de tels lieux, les entrées, fenêtres de domiciles ou tout lieu privé devront être « floutés ».

Les commerçants peuvent être autorisés à filmer la voie publique pour assurer la protection des abords immédiats des bâtiments et installations dans les lieux particulièrement exposés à des risques d'agression ou de vol (article L. 251-2 CSI).

En outre, dans le seul cas de la protection contre des menaces terroristes, des personnes privées peuvent être autorisées à filmer la voie publique, et plus particulièrement les abords immédiats des bâtiments et installations concernés (article L. 223-1 CSI).

La notion d'« abords immédiats » recouvre la portion de trottoir ou de voie publique strictement nécessaire à la protection de l'établissement.

II. Les lieux et établissements ouverts au public

Dans les conditions prévues par la loi, des systèmes de vidéoprotection peuvent également être mis en œuvre dans des lieux ou établissements ouverts au public.

Au sens de la jurisprudence, un lieu ouvert au 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, heures ou causes déterminées » (Cass. crim. 29 juin 1988, 87-85.460). Ainsi, l'acquiescement d'un droit d'entrée ne fait pas obstacle à ce qu'un lieu soit regardé comme ouvert au public (piscine ou cinéma par exemple).

Les locaux à usage d'habitation, que leur accès soit physiquement limité ou non (par un code d'accès par exemple), ne sont pas considérés comme des lieux ouverts au public, tout comme les espaces extérieurs d'une copropriété (parking ou espace vert, par exemple).

Les locaux à usage professionnel ne relèvent pas de la vidéoprotection lorsqu'ils ne sont pas ouverts au public. A l'inverse, les locaux à usage professionnel qui accueillent du public sont considérés comme des lieux ouverts au public. Pour un même lieu de travail, le régime juridique applicable peut donc varier selon l'espace considéré.

Par exemple, les caméras installées à l'intérieur des transports publics collectifs de personnes constituent des systèmes de vidéoprotection, à moins que les espaces considérés soient fermés au public.

Les lieux ouverts au public sont des espaces clos, non couverts ou partiellement couverts. Ils font l'objet d'aménagements pour recevoir du public (CE, 11 décembre 1985, *Ville d'Annecy*, Lebon p. 369). Les établissements ouverts au public sont quant à eux des espaces clos et couverts.

Fiche n°4 : Les personnes qui peuvent être autorisées à installer un système de vidéoprotection

I. Les autorités compétentes

La loi fixe de manière limitative les personnes autorisées à mettre en œuvre un système de vidéoprotection qui sont responsables de système et revêtent la qualité de responsable de traitement au sens du RGPD ou de la loi « informatique et libertés ». Il s'agit :

- Des autorités publiques compétentes pour assurer les finalités prévues à l'article L. 251-2 du code de la sécurité intérieure, qui peuvent être, à titre d'exemple, le maire d'une commune, le dirigeant d'un établissement public (RATP, hôpital, etc.), le responsable d'une administration publique. Dans le cadre de délégation d'attributions, certaines personnes morales peuvent être regardées comme des autorités publiques compétentes. A titre d'exemple, les sociétés concessionnaires d'autoroutes peuvent être regardées comme des autorités publiques en raison de la délégation, par une autorité publique, d'attributions en matière de régulation des flux routiers ;
- De certains commerçants ;
- De certaines autres personnes morales de droit privé (gestionnaires d'un lieu ou établissement ouvert au public particulièrement exposé à des risques d'agression ou de vol et propriétaires de bâtiments et installations dans des lieux susceptibles d'être exposés à des actes de terrorisme).

II. Les finalités de la vidéoprotection

La loi prévoit que la ou les finalités que peut poursuivre le système de vidéoprotection varie selon le lieu de son installation et la qualité de la personne qui le met en œuvre.

1. Sur la voie publique

Sur la voie publique, la vidéoprotection peut être mise en œuvre par les autorités publiques compétentes pour assurer :

- La protection des bâtiments et installations publics et de leurs abords ;
- La sauvegarde des installations utiles à la défense nationale ;
- La régulation des flux de transport ;
- La constatation des infractions aux règles de la circulation ;
- La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières ;
- La prévention d'actes de terrorisme ;
- La prévention des risques naturels ou technologiques ;
- Le secours aux personnes et la défense contre l'incendie ;
- La sécurité des installations accueillant du public dans les parcs d'attraction ;
- Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;
- La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets.

Pour la protection des abords immédiats de leurs bâtiments et installations, les personnes morales de droit privé peuvent être autorisées à mettre en œuvre des systèmes de vidéoprotection dans les lieux susceptibles d'être exposés à des actes de terrorisme.

L'existence d'un risque d'actes de terrorisme s'apprécie au regard des circonstances et du lieu.

Les commerçants peuvent également mettre en œuvre sur la voie publique un système de vidéoprotection aux fins 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. Dans cette hypothèse, les commerçants ne peuvent pas procéder au visionnage des images captées, qui n'est autorisé qu'aux agents des services de police et de gendarmerie nationales, aux agents des services de police municipale ainsi qu'aux agents de la Ville de Paris chargés d'un service de police, aux contrôleurs relevant du statut des administrations parisiennes exerçant leurs fonctions dans la spécialité voie publique et aux agents de surveillance de Paris.

L'existence d'un risque d'agression ou de vol s'apprécie au cas par cas. Peuvent, à titre d'exemple, être retenus pour conclure à l'existence de ce risque : l'isolement ou l'ouverture tardive d'un commerce (centre commercial, station-service), la valeur des marchandises détenues (banque, bijouterie) ou leur nature (pharmacie), le nombre d'agressions ou de vols commis au même endroit ou dans des endroits comparables ou le niveau général de la délinquance dans la ville ou le quartier concerné.

2. Dans les lieux et établissements ouverts au public

Les systèmes de vidéoprotection peuvent être mis en œuvre dans des lieux ou établissements ouverts au public, par les autorités publiques compétentes ou par des personnes morales de droit privé, aux seules fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.

Ces systèmes peuvent également être mis en œuvre dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont susceptibles d'être exposés à des actes de terrorisme.

Personnes	Types de lieux	Fondements juridiques (CSI)	Finalités
Autorités publiques	Voie publique	Article L. 251-2 Article L. 223-1	<p>La protection des bâtiments et installations publics et de leurs abords ; La sauvegarde des installations utiles à la défense nationale ; La régulation des flux de transport ; La constatation des infractions aux règles de la circulation ; La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières ; La prévention d'actes de terrorisme ; La prévention des risques naturels ou technologiques ; Le secours aux personnes et la défense contre l'incendie ; La sécurité des installations accueillant du public dans les parcs d'attraction ; Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ; La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets.</p>
	Lieux et établissements ouverts au public	Article L. 251-2 (avant dernier alinéa) Article L. 223-1 (deuxième alinéa)	<p>Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol. Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme.</p>
	Voie publique (abords immédiats)	Article L. 223-1 (premier alinéa)	<p>Protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme.</p>
Personnes morales de droit privé, y compris les commerçants	Lieux et établissements ouverts au public	Article L. 251-2 (avant dernier alinéa) Article L. 223-1 (deuxième alinéa)	<p>Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol. Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme.</p>
	Voie publique (abords immédiats)	Articles L. 251-2 (dernier alinéa) et R. 252-3-1	<p>Protection des abords immédiats de leurs bâtiments et des installations dans les lieux particulièrement exposés à des risques d'agression ou de vol. Les bâtiments et installations concernés sont : - les lieux ouverts au public où se déroulent les opérations de vente de biens ou de services ; - les lieux où sont entreposés lesdits biens ou marchandises destinés à ces opérations de vente.</p>
Commerçants uniquement	Voie publique (abords immédiats)	Articles L. 251-2 (dernier alinéa) et R. 252-3-1	<p>Protection des abords immédiats de leurs bâtiments et des installations dans les lieux particulièrement exposés à des risques d'agression ou de vol. Les bâtiments et installations concernés sont : - les lieux ouverts au public où se déroulent les opérations de vente de biens ou de services ; - les lieux où sont entreposés lesdits biens ou marchandises destinés à ces opérations de vente.</p>

Fiche n°5 : La demande d'autorisation

Les systèmes de vidéoprotection requièrent une autorisation préalable du préfet dans le département avant d'être déployés.

Pour ce faire, les personnes ou services qui adressent une demande au préfet en ce sens doivent fournir la documentation adéquate dont les composantes peuvent varier en fonction de la nécessité d'une AIPD ou non.

Le responsable d'un système est tenu de déclarer toute modification de son système présentant un caractère substantiel.

I. Contenu de la demande d'autorisation présentée par le responsable du système de vidéoprotection.

- *En l'absence d'une AIPD.*

La demande d'autorisation préalable à l'installation d'un système de vidéoprotection est déposée par le chef de service responsable localement compétent. Elle est accompagnée d'un dossier administratif et technique comprenant les éléments listés ci-dessous.

Contrairement à la procédure antérieure à l'entrée en vigueur du décret n° 2023-1102 du 27 novembre 2023 précité, ce dossier ne comprend plus les consignes générales données aux personnels d'exploitation du système pour le fonctionnement de celui-ci et le traitement des images.

Il doit comprendre en revanche :

- Un **rapport de présentation** : il détaille les finalités pour lesquelles le système de vidéoprotection est installé et les caractéristiques techniques du système mis en œuvre. Le responsable de traitement devra notamment détailler la nature de l'activité exercée et les risques d'agression ou de vol auquel est soumis le lieu ou l'établissement à protéger ;
- Si les systèmes de vidéoprotection portent sur la voie publique, un **plan de masse** des lieux montrant les bâtiments du demandeur et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures, ainsi qu'un **plan de détail** à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci. Ce plan de masse ou de détail peut être remplacé par un **plan du périmètre d'installation du système**, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras, lorsque la demande est relative à l'installation d'un système de vidéoprotection à l'intérieur d'un ensemble immobilier ou foncier complexe ou de grande dimension.
- Lorsque les systèmes de vidéoprotection comportent au moins huit caméras, un **plan de détail** à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci. Ce plan de détail peut être remplacé par un **plan du périmètre d'installation du système**, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras, lorsque la demande est relative à l'installation d'un système de vidéoprotection à l'intérieur d'un ensemble immobilier ou foncier complexe ou de grande dimension.
- Lorsque des raisons d'ordre public et des raisons liées à l'utilisation de dispositifs mobiles de surveillance de la circulation routière s'opposent à la transmission de tout ou partie de certaines indications, ou dans le cas où des raisons impérieuses touchant

à la sécurité des lieux où sont conservés des fonds ou valeurs, des objets d'art ou des objets précieux s'opposent à la transmission par le demandeur de la totalité des informations contenues dans le plan de détail, le dossier de demande d'autorisation peut justifier l'absence du plan de masse ou du plan de détail ;

- Lorsque les commerçants peuvent mettre en œuvre sur la voie publique un système de vidéoprotection aux fins 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, le plan de détail doit montrer la zone couverte par la ou les caméras dont le champ de vision doit être limité aux abords immédiats des bâtiments et installations en cause ;
- La description du **dispositif prévu pour la transmission, l'enregistrement et le traitement des images** ;
- La description des **mesures de sécurité prises pour la sauvegarde et la protection des images** éventuellement enregistrées : le responsable de traitement doit détailler comment est garantie la sécurité de l'exploitation, du réseau informatique, comment sont protégées les images contre les logiciels malveillants, comment l'accès aux images est protégé (local sous contrôle d'accès physique, connexion par mot de passe), comment la maintenance du système est effectuée ;
- Les modalités de **l'information du public** (se référer à la fiche n° 1-B sur ce point) ;
- **Le délai de conservation des images** souhaité, s'il y a lieu, avec les justifications nécessaires. Ce délai sera fixé par l'autorisation préfectorale et ne peut excéder un mois ;
- La **désignation du responsable de la maintenance**, s'il s'agit d'une personne ou d'un service différent de la personne ou du service responsable du système ;
- Les modalités du **droit d'accès** des personnes intéressées ;
- **La justification de la conformité du système de vidéoprotection aux normes techniques** définies par arrêté en application de l'article L. 252-4 du code de la sécurité intérieure⁸ ;
- Le cas échéant, **l'engagement de conformité** destiné à la CNIL (se référer à la fiche n° 1-B sur ce point).

- *En présence d'une AIPD.*

Lorsqu'une AIPD a été rédigée, elle est jointe à la demande d'autorisation et remplace les éléments du dossier suivants :

- le rapport de présentation ;
- la description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images ;
- la description des mesures de sécurité prises pour la sauvegarde et la protection des images éventuellement enregistrées ;

⁸ Un modèle d'attestation est proposé dans la notice d'information relative au formulaire CERFA n° 13806*03 (annexe 5). Cette notice est en cours d'actualisation mais peut continuer à être utilisée dans l'attente de la publication d'une nouvelle version.

- les modalités d'information du public ;
- la précision du délai de conservation des images ;
- la désignation du responsable de la maintenance ;
- les modalités du droit d'accès des personnes intéressées.

Lorsqu'il a rédigé une AIPD, le demandeur a la possibilité, lors de la complétion du formulaire CERFA n° 13806*04, d'opérer des renvois à son AIPD pour les champs pertinents.

II. Le lieu de dépôt de la demande d'autorisation par le responsable du système de vidéoprotection

Le dossier de demande d'autorisation doit être déposé à la préfecture du département du lieu d'implantation des caméras ou, à Paris et sur les emprises des aérodromes de Paris-Charles de Gaulle, Paris-Le Bourget et Paris-Orly, à la préfecture de police de Paris et, dans le département des Bouches-du-Rhône, à la préfecture de police des Bouches-du-Rhône.

Lorsque le système comporte des caméras installées sur le territoire de plusieurs départements, la demande est déposée à la préfecture du département du siège social du demandeur ou, si le siège social du demandeur est situé à Paris, à la préfecture de police, et, s'il est situé dans le département des Bouches-du-Rhône, à la préfecture de police des Bouches-du-Rhône. Cette hypothèse concerne uniquement les systèmes de vidéoprotection qui ont vocation à être déployés de manière continue sur le territoire de plusieurs départements (exemple : un bus équipé de caméras intérieures qui traverse plusieurs départements). A l'inverse, si une même entreprise dispose d'établissements dans plusieurs départements, les systèmes de vidéoprotection doivent être considérés distincts et faire l'objet de demandes d'autorisation dans chaque département.

Le fait que le dispositif comporte un centre de traitement des images éloigné de ce lieu n'affecte pas la compétence du préfet du lieu d'implantation des caméras.

Le dépôt d'un dossier, dès lors que celui-ci est complet, donne lieu à délivrance d'un récépissé qui fixe le point de départ des délais légaux. Le dossier est réputé complet lorsqu'il comporte l'ensemble des documents requis par l'article R. 252-3 du code de la sécurité intérieure et que les informations fournies au titre d'une catégorie de documents sont suffisamment précises. Le caractère limitatif de la liste des informations ne fait en effet pas obstacle à ce que le préfet demande des précisions utiles, y compris sous forme de documents complémentaires.

Lorsque la demande porte sur la mise en œuvre de caméras mobiles installées dans des véhicules, le préfet compétent sera celui du lieu du siège de la personne responsable du système.

Fiche n° 6 : Le rôle de la commission départementale de vidéoprotection

La commission départementale de vidéoprotection est instituée par arrêté préfectoral. Il appartient au préfet dans le département de veiller à sa composition et à son bon fonctionnement.

Elle doit être consultée dans le cadre de la procédure d'autorisation d'un système de vidéoprotection. Elle rend un avis simple, qui ne lie donc pas l'autorité administrative. Dans le cadre de sa mission consultative, elle examine la régularité et la proportionnalité du dispositif envisagé.

Les attributions de cette commission sont exercées, sur les emprises des aérodromes de Paris-Charles de Gaulle, Paris-Le Bourget et Paris-Orly, par la commission départementale de vidéoprotection de Paris.

I. Composition

La commission est composée de quatre membres désignés pour trois ans, chacun ayant un suppléant :

- Un magistrat du siège honoraire, ou, à défaut, une personnalité qualifiée à raison de sa compétence dans le domaine de la vidéoprotection ou des libertés individuelles désignée par le premier président de la cour d'appel, qui la préside ;
- Un maire, désigné par la ou les associations départementales des maires, ou, à Paris, un conseiller de Paris ou conseiller d'arrondissement désigné par le Conseil de Paris ;
- Un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes ;
- Une personnalité qualifiée choisie par le préfet en raison de sa compétence.

Dans le cas où il existe plusieurs associations des maires ou plusieurs chambres de commerce et de l'industrie, le préfet dans le département invite leurs présidents à rechercher un accord sur un seul nom pour ce qui concerne le titulaire et le suppléant. Si un tel accord ne peut être obtenu, le préfet dans le département choisit le représentant de ces associations ou organismes parmi les candidatures qui lui ont été soumises.

La personnalité qualifiée, désignée par le préfet, doit être choisie en raison de sa compétence dans un domaine présentant un lien avec la vidéoprotection : connaissance de la technique employée, compétence dans le domaine de la sécurité publique ou des droits fondamentaux. Cette personnalité qualifiée ne saurait être un agent public en fonction dans les services préfectoraux ou dans les services de police ou de gendarmerie.

II. Fonctionnement

La commission départementale est consultée préalablement à toute décision préfectorale sur les demandes d'autorisation de systèmes de vidéoprotection et de modification de systèmes existants, à l'exception de ceux concernant la défense nationale et en cas d'urgence (voir point C).

Son secrétariat, désigné par le préfet, est assuré par un agent de la préfecture.

A. L'instruction des demandes par la commission départementale de vidéoprotection

La commission peut entendre le demandeur, solliciter tout complément d'information sur les pièces du dossier et, le cas échéant, solliciter l'avis de toute personne qualifiée qui lui paraîtrait indispensable pour l'examen d'un dossier particulier. Elle est, en tout état de cause, tenue d'entendre un représentant de la police ou de la gendarmerie nationales territorialement compétent ou un agent des douanes ou des services d'incendie et de secours ou un représentant de la police municipale concernée. Cette audition d'un responsable de la sécurité joue un rôle déterminant dans l'appréciation que la commission porte sur l'intérêt qui s'attache à l'implantation d'un dispositif. Elle permet à cette dernière d'exercer le contrôle de proportionnalité qui se trouve au centre de sa mission.

B. Les modalités de consultation de la commission départementale de vidéoprotection

La commission doit émettre son avis dans un délai de trois mois. A l'issue de ce délai, si la commission départementale n'a pas émis d'avis, cet avis est réputé donné.

Toutefois, avant l'expiration de ce délai, la commission siégeant en formation plénière peut demander à disposer d'un délai supplémentaire d'un mois, dont l'octroi est de droit.

La réglementation n'organise aucune mesure de publicité de l'avis de la commission ni sa transmission au demandeur. Saisi d'une demande tendant à la communication d'un avis, le préfet doit en apprécier le bien-fondé au regard des règles relatives à la communication des documents administratifs prévue par le code des relations entre le public et l'administration (CRPA). Cet avis est un document produit par une commission administrative dans le cadre d'une mission de service public. A ce titre, il est en principe communicable. Il se peut cependant, dans certains cas, qu'un avis comporte des mentions dont la divulgation porterait atteinte à la sûreté de l'Etat, à la sécurité publique ou à celle des personnes, ou compromettrait un secret protégé par la loi (secret de la vie privée, secret médical, secret professionnel, secret en matière commerciale et industrielle...). Pour préserver la confidentialité des informations protégées, l'administration peut communiquer un document en occultant certains passages.

De façon générale, les membres de la commission doivent s'abstenir de communiquer la teneur de ses avis à des tiers ou de faire état des informations qui auront pu être portées à leur connaissance. De telles divulgations pourraient en effet compromettre la sécurité des lieux et établissements concernés. Cette obligation de discrétion professionnelle doit être rappelée à tous les membres de la commission.

C. L'absence de consultation de la commission départementale de vidéoprotection en cas d'urgence

Dans certains cas d'urgence, le préfet a la faculté de prendre un arrêté d'autorisation d'installation d'un système de vidéoprotection sans avis préalable de la commission départementale, pour une durée maximale de quatre mois.

Cette procédure exceptionnelle vise à accélérer le traitement de deux types de situations :

- les demandes présentées par des pétitionnaires exposés de manière soudaine à des risques terroristes ;
- les manifestations ou rassemblements de grande ampleur dont le préfet est informé dans un délai trop bref pour réunir la commission départementale de

vidéoprotection. Les événements visés par cette procédure d'autorisation provisoire sont ceux présentant un risque particulier pour la sécurité des personnes et des biens en raison du nombre de personnes attendues et/ou de la nature de la manifestation.

Dans ces cas d'urgence, le président de la commission départementale doit être informé sans délai, par le préfet, de sa décision d'appliquer cette procédure d'urgence. Celui-ci aura alors la possibilité de réunir la commission pour qu'elle donne un avis sur la mise en œuvre de cette procédure. Contrairement à la procédure de droit commun, cet avis interviendra postérieurement à l'arrêté d'autorisation provisoire et seulement si la manifestation ou le rassemblement n'a pas encore pris fin.

Si le demandeur souhaite maintenir son dispositif après l'expiration du délai de quatre mois, il devra présenter une demande d'autorisation, qui sera instruite selon la procédure de droit commun. La délivrance d'une autorisation provisoire ne préjugera pas nécessairement du sens de la décision statuant sur cette demande, qui pourra tenir compte d'éléments portés à la connaissance du préfet postérieurement à cette délivrance.

Fiche n° 7 : La décision préfectorale

Ces éléments n'ont pas été modifiés par la loi du 19 mai 2023.

I. Le travail d'instruction préfectorale relative à une demande d'autorisation de déploiement d'un système de vidéoprotection.

Avant d'autoriser le déploiement d'un système de vidéoprotection, le préfet instruit le dossier qui lui a été soumis.

Lorsque le préfet est saisi de demandes relatives à la vidéoprotection sur la voie publique ou dans des lieux et établissements ouverts au public, il vérifie, compte tenu de la nature du lieu surveillé, des finalités poursuivies et des autorités ou personnes morales concernées, la régularité de la demande qui est présentée (cf. fiche n° 5).

Selon les considérations mises en avant par le demandeur, il examine les trois points suivants.

a) Le cas échéant, le lieu est-il particulièrement exposé à des risques d'agression ou de vol ?

Pourront, à titre d'exemple, être retenus pour conclure à l'existence de ce risque :

- l'isolement ou l'ouverture tardive d'un commerce (centre commercial, station-service) ;
- la valeur des marchandises détenues (banque, bijouterie) ou leur nature (pharmacie) ;
- le nombre d'agressions ou de vols commis au même endroit ou dans des endroits comparables ;
- le niveau général de la délinquance dans la ville ou le quartier concerné.

L'intérêt de la vidéoprotection en termes de prévention de la délinquance doit conduire à considérer que ce risque est avéré, dans certains cas, alors même que le lieu ou l'établissement à surveiller n'a pas, au jour de la demande, connu d'agression ou de vol. Il appartient au service de sécurité territorialement compétent de fournir, lors de son audition par la commission départementale, les informations relatives au niveau de risque dans le type d'établissement ou dans le quartier concerné.

b) Le lieu est-il soumis à une menace terroriste ?

Cette condition pourra notamment être tenue pour remplie si le dispositif a pour vocation de protéger des lieux emblématiques d'institutions publiques, de certains groupes ou intérêts faisant notoirement l'objet de menaces, des lieux dans lesquels une éventuelle attaque aurait un retentissement particulier en raison du nombre des victimes potentielles ou du public concerné (ex : lieux de culte). Elle pourra également l'être lorsque sont en cause des lieux couverts par un plan de sécurité prévu par le code de la défense ou par une norme de niveau européen.

c) Le contrôle de proportionnalité.

Le préfet est chargé de veiller à ce que les systèmes de vidéoprotection ne portent pas une atteinte excessive au droit de chacun au respect de sa vie privée, au regard de l'intérêt qu'ils présentent en termes de sécurité ou d'ordre public. Il exerce donc un contrôle de proportionnalité qui constitue le cadre traditionnel d'appréciation des mesures de police administrative, au regard du deuxième alinéa de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales qui impose le respect du droit à la vie privée. Différents éléments sont susceptibles de guider son appréciation en la matière (nécessité avérée de la vidéoprotection, ampleur du dispositif, etc.).

II. La décision d'autorisation

A. Le contenu de la décision d'autorisation.

L'autorisation préfectorale est délivrée pour une durée de cinq ans renouvelable.

L'autorisation précise les précautions utiles, en particulier le délai de conservation des images issues des systèmes de vidéoprotection, les personnes chargées de l'exploitation du système de vidéoprotection, les mesures à prendre pour assurer le respect des dispositions du code de la sécurité intérieure, notamment pour être conformes aux normes techniques définies par arrêté en application de l'article L. 252-4 du code de la sécurité intérieure.

Concernant le délai de conservation des images par le responsable du système, il ne peut excéder un mois. Au terme de ce délai, les données doivent être effacées automatiquement des traitements. À l'inverse, l'autorisation préfectorale peut prévoir un délai minimal de conservation des enregistrements.

Lorsque les données ont, dans ce délai, été extraites et transmises pour les besoins d'une procédure judiciaire, administrative ou disciplinaire, elles sont conservées selon les règles propres à chacune de ces procédures par l'autorité qui en a la charge.

L'autorisation doit également préciser les personnes pouvant accéder au visionnage des images, et celles pouvant en être destinataires. Il n'est pas nécessaire que l'autorisation comporte les noms des agents des services concernés. Elle indiquera seulement les catégories de personnes concernées, parmi celles listées à l'article R. 253-3 du code de la sécurité intérieure. La désignation revient donc aux services concernés. L'accès peut être autorisé pour la totalité de la durée de validité de l'autorisation ou pour une période plus réduite, correspondant, par exemple, au déroulement d'un évènement précisément identifié.

Le tableau ci-dessous recense les personnes qui, en application de l'article R. 253-3 du code de la sécurité intérieure, peuvent visionner les images issues des systèmes de vidéoprotection mis en œuvre.

Par ailleurs, pourront recevoir communication des images issues d'un système de vidéoprotection mis en œuvre par un tiers service ou une tierce personne, en application du III de l'article R. 253-3 du CSI :

- Les agents des services de police nationale ;
- Les agents des unités de la gendarmerie nationale ;
- Les agents des douanes ;
- Les agents des services d'incendie et de secours ;
- Les agents de police municipale pour les seules images issues de systèmes implantés sur le territoire de la commune ou de l'établissement public de coopération intercommunale dont ils relèvent ;
- Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1 pour les seules images issues de systèmes implantés sur le territoire de la ville de Paris ;
- Les autorités administratives et judiciaires dont la présence est requise dans les salles de commandement au sein desquelles des images de vidéoprotection sont transmises ;
- Les officiers et agents de police judiciaire ;
- Les agents des services d'inspection générale de l'Etat.

Responsable du système de vidéoprotection	Lieux de mise en œuvre du système	Accédants	
Autorité publique	Voie publique	<p>Autorités publiques (hors communes)</p> <p>Les agents individuellement désignés et dûment habilités par les autorités publiques responsables du système.</p> <p>Communes</p> <p>Le maire ;</p> <p>Les adjoints au maire et membres du conseil municipal qui sont délégués d'attributions de police municipale ;</p> <p>Les agents de police municipale ;</p> <p>Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1 ;</p> <p>Les agents des communes, des établissements publics de coopération intercommunale et des syndicats mixtes, agréés par le représentant de l'Etat dans le département, en application de l'article L. 132-14-1 du code de la sécurité intérieure.</p>	
	Lieux et établissements ouverts au public	<p>Les agents qui relèvent de l'autorité publique individuellement désignés et dûment habilités par elle ;</p> <p>Les opérateurs privés agissant pour le compte de la personne morale, en application de l'article L. 613-13.</p>	
Personne morale de droit privé, hors commerçants	Voie publique (abords immédiats des bâtiments et installations <u>dans les lieux susceptibles d'être exposés à des actes de terrorisme uniquement</u>)	<p>Les opérateurs relevant de la personne morale individuellement désignés et dûment habilités par elle ;</p> <p>Les opérateurs privés agissant pour le compte de la personne morale, en application de l'article L. 613-13.</p>	
	Lieux et établissements ouverts au public	<p>Les agents qui relèvent de la personne morale individuellement désignés et dûment habilités par elle ;</p> <p>Les opérateurs privés agissant pour le compte du responsable du système, dans les conditions prévues à l'article L. 613-13.</p>	
Commerçants	Voie publique (abords immédiats des bâtiments et installations)	Dans les lieux particulièrement exposés à des risques d'agression ou de vol	<p>Les agents des services de police nationale ;</p> <p>Les agents des unités de la gendarmerie nationale ;</p> <p>Les agents de police municipale ;</p> <p>Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1.</p>
		Dans les lieux susceptibles d'être exposés à des actes de terrorisme uniquement	<p>Les opérateurs relevant du commerçant individuellement désignés et dûment habilités par lui ;</p> <p>Les opérateurs privés agissant pour le compte du commerçant, en application de l'article L. 613-13.</p>
	Lieux et établissements ouverts au public	<p>Les opérateurs qui relèvent du commerçant individuellement désignés et dûment habilités par lui ;</p> <p>Les opérateurs privés agissant pour le compte du commerçant, dans les conditions prévues à l'article L. 613-13.</p>	

B. Obligations procédurales encadrant la décision préfectorale.

Le silence gardé par le préfet pendant plus de quatre mois sur une demande d'autorisation vaut décision de rejet.

En application de l'article L. 211-2 du code des relations entre le public et l'administration, les décisions défavorables doivent être motivées.

L'autorisation doit être publiée au recueil des actes administratifs de la préfecture, sauf dérogation motivée par un impératif de défense nationale. Le préfet met à la disposition du public la liste des autorisations de systèmes de vidéoprotection publiées dans les conditions prévues à l'article R. 252-16 du code de la sécurité intérieure, qui précise pour chacun d'eux la date de son autorisation et le service ou la personne responsable. Il communique également la liste des systèmes de vidéoprotection autorisés sur le territoire de chaque commune au maire, qui la met à la disposition du public à la mairie et, le cas échéant, dans les mairies d'arrondissement.

III. L'autorisation provisoire

Lorsque l'urgence et l'exposition particulière à un risque d'acte de terrorisme le requièrent, le préfet peut délivrer aux autorités publiques compétentes ou aux personnes morales, sans avis préalable de la commission départementale de vidéoprotection, une autorisation provisoire d'installation d'un système de vidéoprotection, pour une durée maximale de quatre mois.

De même, lorsqu'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens, il peut également délivrer, à ces mêmes personnes, sans avis préalable de la commission départementale de vidéoprotection, une autorisation provisoire d'installation d'un système de vidéoprotection, pour une durée maximale de quatre mois.

Dans ces deux hypothèses, le préfet informe immédiatement le président de la commission départementale de vidéoprotection, qui peut la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure d'autorisation provisoire.

Le préfet recueille l'avis de la commission départementale de vidéoprotection sur la mise en œuvre du système de vidéoprotection et se prononce sur son maintien. La commission doit rendre son avis avant l'expiration du délai de validité de l'autorisation provisoire.

IV. La prescription préfectorale

Le préfet peut prescrire la mise en œuvre de systèmes de vidéoprotection dans trois situations.

Aux fins de prévention d'actes de terrorisme, il peut prescrire la mise en œuvre, dans un délai qu'il fixe, de systèmes de vidéoprotection, aux personnes suivantes :

- Les exploitants, publics ou privés, des établissements, installations ou ouvrages, désignés par l'autorité administrative, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, au sens des articles L. 1332-1 et 1332-2 du code de la défense, ainsi que les exploitants de certains établissements, en application de l'article L. 1332-2 du code de la défense⁹ ;

⁹ Usines, ateliers, dépôts, chantiers et, d'une manière générale, les installations exploitées ou détenues par toute personne physique ou morale, publique ou privée, qui peuvent présenter des dangers ou des inconvénients soit pour la commodité du voisinage, soit pour la santé, la sécurité, la salubrité publiques, soit pour l'agriculture, soit pour la

- Les gestionnaires d'infrastructures, les autorités et personnes exploitant des transports collectifs, relevant de l'activité de transports terrestres qui s'effectuent entre un point d'origine et un point de destination situés sur le territoire national, en application de l'article L. 1000-1 du code des transports ;
- Les exploitants d'aéroports qui sont ouverts au trafic international.

Cette prescription préfectorale doit être précédée, sauf en matière de défense nationale, d'une consultation de la commission départementale de vidéoprotection si elle porte sur une installation de vidéoprotection filmant la voie publique ou des lieux et établissements ouverts au public.

De plus, lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, il peut également prescrire, sans avis préalable de la commission départementale de vidéoprotection, la mise en œuvre d'un système de vidéoprotection.

Enfin, lorsqu'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens, il peut prescrire, sans avis préalable de la commission départementale de vidéoprotection, la mise en œuvre d'un système de vidéoprotection.

Dans ces deux dernières hypothèses, le président de la commission est immédiatement informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure de décision provisoire.

Avant l'expiration d'un délai maximal de quatre mois, le préfet recueille l'avis de la commission départementale de vidéoprotection sur la mise en œuvre du système de vidéoprotection et se prononce sur son maintien.

V. La demande de mise en œuvre d'un système

Aux fins de prévention d'actes de terrorisme, de protection des abords des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ou de protection des intérêts fondamentaux de la Nation, le préfet peut demander à une commune la mise en œuvre de systèmes de vidéoprotection. Le conseil municipal doit alors délibérer dans un délai de trois mois sur cette demande. En cas de décision positive, la commune doit réaliser une demande d'autorisation de mise en œuvre d'un système de vidéoprotection, dans les conditions exposées dans la fiche n° 5 de la présente circulaire, pour une ou plusieurs finalités visées à l'article L. 251-2 du code de la sécurité intérieure.

Les conditions de financement du fonctionnement et de la maintenance du système de vidéoprotection font l'objet d'une convention conclue entre la commune de son lieu d'implantation et le préfet.

VI. La procédure de modification des demandes

Lorsque des modifications apportées à un système sont portées à la connaissance du préfet, il doit évaluer la nécessité de délivrer une nouvelle autorisation au responsable de système.

protection de la nature, de l'environnement et des paysages, soit pour l'utilisation économe des sols naturels, agricoles ou forestiers, soit pour l'utilisation rationnelle de l'énergie, soit pour la conservation des sites et des monuments ainsi que des éléments du patrimoine archéologique, ainsi que les exploitants des établissements comprenant une installation nucléaire de base, à savoir, réacteur nucléaire, installations de préparation, d'enrichissement, de fabrication, de traitement ou d'entreposage de combustibles nucléaires ou de traitement, d'entreposage ou de stockage de déchets radioactifs, installations contenant des substances radioactives ou fissiles et répondant à des caractéristiques définies, accélérateurs de particules répondant à des caractéristiques définies ou les centres de stockage en couche géologique profonde de déchets radioactifs, quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population.

Les modifications nécessitant une nouvelle autorisation préfectorale sont les suivantes :

- la modification de la nature des lieux protégés ;
- la modification des finalités du système ;
- la modification des conditions d'exploitation des images ;
- la modification de la durée de conservation des images ;
- la modification des caractéristiques techniques du système.

Dans d'autres cas, il convient d'apprécier si les modifications apportées au système appellent, compte tenu de leur nature et de leur ampleur, le retrait de l'autorisation et la délivrance d'une nouvelle autorisation. Il y aura place pour une telle appréciation face à une augmentation limitée du nombre des caméras ou de la surface couverte. Il en ira de même dans le cas où un changement dans l'organisation de la personne morale titulaire de l'autorisation survient. A titre d'exemple, un changement radical de la nature de l'activité commerciale dans un local équipé de vidéoprotection devra sans doute conduire le préfet à retirer l'autorisation et à en délivrer une nouvelle.

VII. La procédure de renouvellement des demandes d'autorisation

Dans le cadre de demandes de renouvellement, le demandeur doit déposer un nouveau dossier complet.

S'agissant des demandes de renouvellement d'autorisation de systèmes de vidéoprotection inchangés depuis leur autorisation, une attention particulière doit être portée au contexte du site dans lequel le système est installé, celui-ci ayant pu évoluer (réalisation d'aménagements urbains, évolution du risque d'atteinte aux biens ou aux personnes, etc.). Quels que soient le nombre de caméras et la nature des lieux visionnés, les services de préfecture doivent avoir communication des documents relatifs au contexte ayant évolué depuis la demande d'autorisation initiale.

Même si le système de vidéoprotection est inchangé, son autorisation doit être renouvelée après avis de la commission départementale.

Enfin, si les titulaires d'autorisations venues à échéance ne sollicitent pas une demande de renouvellement, le préfet peut considérer l'autorisation délivrée comme caduque.

Fiche n° 8 : Les contrôles et sanctions

I. Le contrôle de la commission départementale de vidéoprotection

Dans le cadre des contrôles qu'elle exerce de sa propre initiative ou sur saisine de toute personne intéressée, la commission départementale de vidéoprotection peut déléguer un de ses membres pour collecter, notamment auprès du responsable du système, les informations utiles relatives aux conditions de fonctionnement d'un système de vidéoprotection et visant à vérifier le respect des obligations de destruction des enregistrements ou la conformité du système à son autorisation.

La commission départementale de vidéoprotection peut être réunie à l'initiative de son président pour examiner les résultats des contrôles et émettre, le cas échéant, des recommandations et proposer au préfet la suspension ou la suppression d'un système de vidéoprotection lorsqu'elle constate qu'il n'est pas autorisé ou qu'il en est fait un usage anormal ou non conforme à son autorisation.

La commission départementale de vidéoprotection exerce sa mission de contrôle dans les conditions prévues par l'article L. 253-3 du code de la sécurité intérieure.

II. Le contrôle de la CNIL

Avant l'entrée en vigueur de la loi du 19 mai 2023, les pouvoirs de la CNIL étaient déterminés par le code de la sécurité intérieure. Désormais, elle exerce ses prérogatives conformément à la loi « informatique et libertés ».

La CNIL peut contrôler tout responsable de traitement à la suite de plaintes qu'elle reçoit, de signalements qui lui sont faits, ou sur simple auto-saisine. Ces contrôles peuvent avoir lieu sur place, en ligne ou constituer une audition sur convocation.

En cas de manquements constatés lors du contrôle, le président de la CNIL peut décider d'une mise en demeure ou la formation restreinte peut prononcer différentes mesures ou sanctions.

III. Le contrôle du préfet

Le préfet peut faire procéder, par les services de police ou de gendarmerie, à des contrôles de vérification des prescriptions émises dans les autorisations préfectorales. Le contrôle peut également porter sur l'existence de systèmes non autorisés et sur la conformité du système aux normes techniques définies par arrêté en application de l'article L. 252-4 du code de la sécurité intérieure.

L'article R. 252-17 du code de la sécurité intérieure impose au responsable du système de tenir le préfet informé des événements importants qui affectent l'exploitation du système de vidéoprotection mis en œuvre. Doivent à ce titre lui être signalés la mise en service effective des caméras, ainsi que la localisation des caméras à l'intérieur du périmètre d'installation du système de vidéoprotection préalablement à leur installation et, le cas échéant, à leur déplacement.

IV. Les sanctions

A. La suspension de l'autorisation

A l'issue du contrôle qu'elle peut exercer sur les systèmes de vidéoprotection, la commission départementale de vidéoprotection peut, après en avoir informé le maire, proposer au préfet la suspension de l'autorisation d'installation, en application de l'article L. 253-1 du code de la sécurité intérieure.

L'interruption provisoire de la mise en œuvre du traitement peut être prononcée pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III lorsqu'ils sont mis en œuvre pour le compte de l'Etat. Concernant le cas spécifique de ces derniers, la CNIL peut informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée. Le Premier ministre fait alors connaître à la formation restreinte de la CNIL les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

B. Le retrait de l'autorisation

A l'issue du contrôle qu'elle peut exercer sur les systèmes de vidéoprotection, la commission départementale de vidéoprotection peut, après en avoir informé le maire, proposer au préfet le retrait de l'autorisation d'installation, en cas de manquement à la loi ou de modification des conditions au vu desquelles elle a été délivrée.

C. La fermeture administrative de l'établissement

Le maintien d'un système de vidéoprotection sans autorisation peut entraîner, après mise en demeure du préfet, la fermeture administrative de l'établissement pour une durée de trois mois, par décision du préfet, à la demande de cette commission ou de sa propre initiative, en application de l'article L. 253-4 du code de la sécurité intérieure. A l'issue de cette période de trois mois, si l'établissement n'a pas régularisé sa situation, le préfet peut lui enjoindre de démonter ledit système et, s'il ne donne pas suite à cette injonction, prononcer une nouvelle mesure de fermeture de trois mois.

D. Sanction pénale

La mise en œuvre d'un système de vidéoprotection fixant, enregistrant ou transmettant l'image d'une personne dans un lieu privé constitue un délit en application de l'article 226-1 du code pénal, puni d'un an d'emprisonnement et de 45 000 euros d'amende.

La mise en œuvre d'un système de vidéoprotection sur la voie publique ou dans un espace ouvert au public sans autorisation préalable constitue un délit en application de l'article 226-16 du code pénal, ce qui peut fonder une saisine du parquet compétent au titre de l'article 40 du code de procédure pénale. Ainsi, les personnes déclarées responsables pénalement d'un tel délit encourent cinq ans d'emprisonnement et 300 000 euros d'amende. Aussi, s'agissant des personnes morales, lorsqu'elles sont déclarées responsables pénalement d'un tel délit, elles encourent les peines auxquelles il est fait référence à l'article 226-24 du code pénal¹⁰.

¹⁰ Il s'agit des peines suivantes : l'amende au quintuple ; l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ; le placement, pour une durée de cinq ans au plus, sous surveillance judiciaire ; la fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; l'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ; l'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le

Ainsi, les personnes déclarées responsables pénalement d'un tel délit encourent un an d'emprisonnement et 45 000 euros d'amende. De même, s'agissant des personnes morales, lorsqu'elles sont déclarées responsables pénalement d'un tel délit, elles encourent les peines prévues à l'article 226-7 de ce même code¹¹.

retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ; la peine de confiscation, dans les conditions et selon les modalités prévues à l'article 131-21 ; l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

¹¹ Il s'agit des peines suivantes : l'amende au quintuple ; l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ; l'affichage ou la diffusion de la décision prononcée, dans les conditions prévues par l'article 131-35.