VIDÉOPROTECTION

Le LIVRE BLANC au service des ÉLUS et des FUTURS ÉLUS



CONCILIER SÉCURITÉ, EFFICACITÉ et LIBERTÉS PUBLIQUES.



ÉDITORIAL

Depuis plus de vingt ans, **l'AN2V et ses membres** observent, analysent et confrontent la réalité des usages de la vidéoprotection sur le terrain, loin des slogans et des procès d'intention. Créée en 2004 par Dominique Legrand, elle s'est construite comme un espace de travail exigeant entre collectivités, services de l'État, industriels et experts, avec une ligne claire : partir des contraintes réelles des élus locaux, du droit en vigueur et des capacités opérationnelles effectives.

À l'heure où les débats sur l'IA, la vidéoprotection et la sécurité publique se crispent, l'AN2V assume un rôle de tiers de confiance. Ni prescripteur technologique, ni acteur militant, elle met en perspective ce qui est possible, ce qui est interdit et ce qui relève encore du fantasme. Elle rappelle que les technologies ne valent que par les usages que l'on en fait, la gouvernance que l'on met en place et les limites que l'on s'impose collectivement.



Ce Livre blanc s'inscrit dans cette continuité. Il ne cherche pas à convaincre par l'émotion mais à outiller par la méthode. Il propose aux équipes municipales une lecture lucide du mandat 2026-2032, en distinguant ce qui peut être déployé dès aujourd'hui à droit constant, ce qui doit être préparé et ce qui ne relève pas du champ démocratiquement acceptable. C'est une contribution pragmatique au débat public, au service de décisions éclairées et responsables.

Dominique LEGRAND - président fondateur de l'AN2V - Association Nationale de la Vidéoprotection
Tiers de confiance des acteurs publics et privés de la sûreté électronique

Vidéoprotection, centres de supervision urbains (CSU) et Remontée Automatique d'Alerte (R2A) : des outils concrets pour aider les communes à prévenir, protéger et intervenir plus vite. À l'approche des municipales 2026, 76% des Français citent la sécurité des personnes et des biens comme un enjeu déterminant (Ifop pour La Tribune Dimanche, 15 novembre 2025).

Ce LIVRE BLANC propose une trajectoire 2026-2032 pour déployer une vidéoprotection utile et une R2A qui détecte des situations, pas des identités, avec des limites connues et contrôlées.



Cette démarche prolonge la mission parlementaire que le Premier ministre Jean Castex m'a confiée le 23 avril 2021, dans la perspective de la protection des grands événements, dont Paris 2024. Aujourd'hui, je poursuis ce travail comme Président de Via Publica Conseils.

Jean-Michel MIS - président de Via Publica Conseils
Ancien député - Missionné par le Premier ministre Jean Castex

TRAVAIL COLLECTIF DES MEMBRES DE L'AN2V

CE LIVRE BLANC EST LE FRUIT D'UN TRAVAIL COLLECTIF MENÉ EN CETTE FIN D'ANNÉE 2025 PAR LES MEMBRES DE L'AN2V.

LEUR ENGAGEMENT, LEUR DISPONIBILITÉ ET LA QUALITÉ DES ÉCHANGES ONT PERMIS DE CONFRONTER LES POINTS DE VUE, D'ENRICHIR LES ANALYSES ET DE RESTER FIDÈLES À CE QUI FAIT L'IDENTITÉ DE L'ASSOCIATION DEPUIS SON ORIGINE : PARTIR DES CONTRAINTES RÉELLES DES ÉLUS LOCAUX, DU DROIT EN VIGUEUR ET DES CAPACITÉS OPÉRATIONNELLES NÉCESSAIRES SUR NOS TERRITOIRES.

PAR ORDRE ALPHABÉTIQUE !



SOMMAIRE

Éditorial 3
Travail collectif des **membres de l'AN2V** **4**
Avant-propos : Pourquoi ce livre blanc, pourquoi maintenant ? 8
À qui s'adresse ce document ? 8
Comment le lire en 10 minutes, 30 minutes ou 2 heures (lecture à tiroirs) ? 9
Ce que ce livre blanc n'est pas : ni catalogue techno, ni manifeste militant ! 9

PARTIE 1 : LA RATIONALITÉ DE LA VIDÉOPROTECTION

Lecture rapide : de la rationalité dans le débat sur la vidéoprotection 10

1.Le mandat 2026–2032 vu d'un maire 12
1.1. Les responsabilités réelles du maire en matière de sécurité et de tranquillité publique 12
1.2. Ce que les habitants attendent vraiment, et ce qu'ils confondent 12
1.3. Pourquoi la vidéoprotection devient un sujet électoral récurrent, même quand elle n'est pas la solution 13

2. Ce qu'est réellement la vidéoprotection aujourd'hui 13
2.1. Vidéosurveillance, vidéoprotection, CSU, CSUi, CSD : mettre fin aux confusions 13
2.2. À quoi sert une caméra, et à quoi elle ne sert jamais 14
2.3. La vidéoprotection comme outil parmi d'autres, pas comme réponse globale 15
3. Le cadre juridique et institutionnel à connaître avant de décider 16
3.1. Le Code de la sécurité intérieure et les 11 finalités de l'article L251-2 16
3.2. Qui fait quoi : maire, préfet, référent sûreté, forces de sécurité intérieure 16
3.3. Espaces publics, bâtiments municipaux, espaces privés ouverts au public : ce que cela change concrètement 17

4. Trois critiques, trois réponses : cher, liberticide, inefficace 17
4.1. « C'est cher » - coût réel, coût évité, mutualisation, arbitrage avec d'autres dépenses 17
4.2. « C'est liberticide » - ce qui est interdit, ce qui est encadré, ce qui est maîtrisable localement 18
4.3. « C'est inefficace » - ce que montrent les retours d'expérience, où la caméra ne sert à rien, où elle change vraiment la donne 18

5. Vidéoprotection utile : principes, lignes rouges et responsabilités politiques 20
5.1. Proportionnalité, ciblage, temporalité : les trois filtres d'un projet défendable 20
5.2. Transparence, information du public, rôle du conseil municipal 20
5.3. Ce qu'une commune responsable s'interdit, même si la technologie le permet 21
5.4. Lancer un projet de vidéoprotection : les choix structurants que le maire ne doit pas déléguer 21

6. Un environnement de menaces et de contraintes profondément renouvelé 22
6.1. Évolution des menaces dans l'espace public : événements, foules, nouvelles vulnérabilités 22
6.2. Ce qui relève du maire, ce qui relève de l'État, ce qu'il est dangereux de promettre .23
6.3. Durcissement réglementaire, judiciarisation et responsabilité des décideurs locaux24
6.4. Anticiper sans suréquiper : préparer le terrain des usages futurs sans changer de nature politique 24

PARTIE 2 : DE LA VIDÉOPROTECTION À LA REMONTÉE AUTOMATIQUE D'ALERTE

Lecture rapide : Comprendre les usages possibles, leurs limites et leurs conditions de déploiement 28

7. De quoi parle-t-on vraiment quand on parle de R2A ? 30
7.1. Pourquoi parle-t-on de Remontée Automatique d'Alerte plutôt que «IA» ou «VSA» ? 30
7.2. Le principe fondamental : détecter des situations, pas des identités 30
7.3. Différence entre vidéosurveillance, vidéoprotection et R2A 31
7.4. Ce que la R2A ne fait pas et ne fera pas dans le cadre juridique européen et national 31
7.5. Synthèse des usages envisageables issus des travaux de l'AN2V 32

8. Dix à quinze cas d'usage prioritaires pour une commune en 2026 32
8.1. Comptage et statistiques 32
8.2. Gestion et optimisation des territoires «connectés et durables» et des espaces publics 33
8.3. Détection de chutes, malaises, noyades et personnes au sol 33
8.4. Départs de feu, fumées anormales et risques dans les équipements 34
8.5. Mouvements de foule, attroupements dangereux, évènements festifs 34
8.6. Sécurité routière : contresens, stationnement dangereux, voies douces 34
8.7. Risques naturels et technologiques : inondations, crues, submersions, incendies 35
8.8. Dépôts sauvages et atteintes à l'environnement 36
8.9. Protection des bâtiments publics sensibles et des abords 36

9. Ce que les collectivités peuvent faire à droit constant dès le début du mandat 37
9.1. Ce que les collectivités peuvent faire à droit constant dès le début du mandat 37
9.2. Les obligations de conformité à intégrer dès la conception 38
9.3. Construire une trajectoire opérationnelle plutôt qu'un empilement d'outils 38
9.4. Exemples de trajectoires opérationnelles dès 2026-2027 selon la taille de la commune 39

10. Ce qui peut réellement évoluer pendant le mandat 2026-2032 41
10.1. IA Act, textes nationaux et travaux interministériels en cours 41
10.2. LAPI : état des lieux, usages existants et perspectives d'ouverture 42
10.3. Rôle des réseaux, référentiels et productions de l'AN2V pendant le mandat 42
10.4. Les futurs grands champs d'usage de la R2A au regard du Code de la sécurité intérieure 43

11. Organisation, ressources humaines et conduite du changement 44
11.1. Passer d'un CSU de «visionnage» à un CSU «piloté par les alertes» : stratégie de «l'écran noir» 44
11.2. Rôle des opérateurs et évolution des compétences 45
11.3. Organisation des procédures, fiches réflexes et chaînes décisionnelles 45
11.4. Articulation entre élus, directions et services : clarifier le «qui fait quoi» 46

12. Encadrement Éthique, maîtrise des risques et acceptabilité démocratique 46
12.1. L'intérêt d'un comité d'éthique local pour sécuriser les décisions 47
12.2. Les risques réels : biais, dépendance industrielle, dérives d'usage, opacité 47
12.3. Les leviers de prévention : gouvernance, contrats, audits et réversibilité 47
12.4. Auditabilité et traçabilité des algorithmes sans entrer dans la boîte noire 48
12.5. Construire un récit public centré sur la prévention, le secours et la résilience 48
12.6. Répondre aux controverses et aux oppositions sans confrontation stérile 48

PARTIE 3 : DÉCIDER, ARBITRER ET ASSUMER SUR LE MANDAT

Lecture rapide : Décider, arbitrer et assumer sur le mandat municipal 52

13. Construire une trajectoire politique crédible sur le mandat 2026-2032 54
13.1. Les six premiers mois 55
13.2. Le cœur du mandat 55
13.3. La fin du mandat 55

14. Adapter sa stratégie… et éviter les erreurs classiques selon la taille de la collectivité 56
14.1. Petites communes 56
14.2. Villes moyennes 56
14.3. Grandes villes et métropoles 57
14.4. Attention à la bonne définition des coopérations 58

15. Sécuriser le projet par les choix administratifs et contractuels 59
15.1. Lorsqu'un projet de vidéoprotection et d'évolution devient un marché public structurant 59
15.2. Les points de vigilance contractuels majeurs 60
15.3. Intégrer dès maintenant les contraintes IA Act, CNIL et CSI 61
15.4. Clauses types et bonnes pratiques contractuelles 61

16. Gouverner, évaluer et rendre compte sans alimenter la défiance 62
16.1. Gouvernance politique et rôle structurant du comité d'éthique 62
16.2. Évaluer sans se noyer dans les indicateurs 62
16.3. Rendre compte régulièrement sans sur-communication 62
16.4. Gérer les oppositions, les recours et les demandes d'accès 63
16.5. Faire de la transparence un levier de confiance 63

LEXIQUE 64

AVANT-PROPOS : POURQUOI CE LIVRE BLANC, POURQUOI MAINTENANT ?

La question de la vidéoprotection et de l'usage de l'intelligence artificielle dans l'espace public n'est ni nouvelle, ni marginale. Elle revient à chaque campagne municipale, souvent sous forme de promesses simplificatrices, de peurs instrumentalisées ou de débats idéologiques qui ignorent volontairement la réalité du terrain. Pourtant, les données disponibles montrent un décalage croissant entre ces représentations et les pratiques réelles des collectivités. Selon une étude récente de l'Institut Quorum pour Orasio, près de neuf communes sur dix de plus de 20 000 habitants envisagent d'accroître leur parc de caméras, et aucune n'envisage de le réduire, signe d'une légitimation désormais acquise de la vidéoprotection de voie publique.
Ce livre blanc est né d'un constat simple. Les élus locaux doivent aujourd'hui prendre des décisions engageantes sur des sujets techniques, juridiques et éthiques complexes, dans un contexte de durcissement réglementaire et de judiciarisation croissante de l'action publique. Dans le même temps, ils sont confrontés à une forte demande de solutions pragmatiques. Toujours selon cette étude, 94,5% des élus et cadres territoriaux se déclarent favorables à l'usage d'outils d'analyse automatisée des images pour des usages concrets et visibles, comme la lutte contre les dépôts sauvages, la protection des sites publics ou la gestion des flux, tout en exprimant des attentes fortes en matière de cadre juridique et de garanties démocratiques.
Pourquoi maintenant ? Parce que le prochain mandat ne ressemblera pas aux précédents. Les textes européens et nationaux encadrant la protection des données et l'intelligence artificielle s'imposent désormais directement aux collectivités. Les menaces évoluent, les attentes citoyennes aussi, mais les marges de manœuvre locales sont plus contraintes qu'hier. À l'approche de 2026, plus de 85% des élus estiment que ces sujets doivent faire l'objet d'un débat local, non comme un pilier de programme, mais comme un marqueur de crédibilité et de capacité à gouverner. Continuer à traiter ces enjeux avec les grilles de lecture du passé serait une erreur.

À QUI S'ADRESSE CE DOCUMENT ?

Ce document s'adresse en priorité aux maires, aux adjoints en charge de la sécurité, de la tranquillité publique ou du numérique, ainsi qu'aux équipes municipales et intercommunales qui participent à la préparation du mandat 2026–2032. Il est conçu pour les élus qui doivent décider, arbitrer et assumer, qu'ils soient novices sur ces sujets ou déjà engagés sur des dispositifs existants.
Il s'adresse également aux directeurs généraux des services, aux responsables des systèmes d'information, aux directeurs de la sécurité, aux juristes et aux cadres territoriaux qui accompagnent les élus dans la structuration et la mise en œuvre des projets. Leur rôle est central, mais il ne peut se substituer à la responsabilité politique du décideur.
Ce livre blanc n'est pas destiné aux spécialistes de l'algorithmie, ni aux acteurs cherchant une validation idéologique de positions préexistantes. Il vise celles et ceux qui acceptent de regarder les sujets de vidéoprotection et de R2A tels qu'ils sont, avec leurs apports réels, leurs limites et leurs risques.

COMMENT LE LIRE EN 10 MINUTES, 30 MINUTES OU 2 HEURES (LECTURE À TIROIRS) ?

Ce livre blanc a été conçu pour une lecture à plusieurs niveaux, afin de s'adapter aux contraintes de temps et aux besoins de chacun.
Une lecture rapide, en quelques minutes, permet de saisir les messages clés, les lignes rouges et les principes structurants à travers les synthèses, encadrés et conclusions de chapitres. Elle est suffisante pour comprendre l'esprit général du document et éviter les contresens majeurs.
Une lecture intermédiaire, en une trentaine de minutes, permet d'acquérir une compréhension solide des enjeux politiques, juridiques et opérationnels. Elle donne les repères nécessaires pour dialoguer utilement avec les services, les partenaires institutionnels et les prestataires, sans se laisser enfermer dans un discours technique.
Une lecture approfondie et détaillée, en deux heures environ, offre une vision complète des usages possibles, des cadres juridiques applicables et des trajectoires réalistes sur un mandat municipal. Elle s'adresse à celles et ceux qui souhaitent structurer une stratégie cohérente et défendable dans la durée.
Enfin, il existe un document PDF de synthèse qui peut se lire en dix minutes, que vous trouverez sur www.an2v.org

CE QUE CE LIVRE BLANC N'EST PAS : NI CATALOGUE TECHNO, NI MANIFESTE MILITANT !

Ce livre blanc n'est ni un catalogue de solutions technologiques, ni un guide d'achat déguisé. Il ne promeut aucune marque, aucun fournisseur, aucun dispositif clé en main. Les technologies évoquées le sont uniquement à travers leurs usages, leurs conditions de déploiement et leurs limites juridiques.
Il n'est pas non plus un manifeste militant, qu'il soit favorable ou hostile à la vidéoprotection et à l'intelligence artificielle. Il ne cherche ni à rassurer par principe, ni à inquiéter pour convaincre. Il part du postulat que les technologies ne sont ni bonnes ni mauvaises en soi, et que seule la manière dont elles sont gouvernées, encadrées et expliquées leur donne un sens démocratiquement acceptable.
Enfin, ce document n'a pas vocation à promettre l'impossible. Il vise au contraire à aider les élus locaux à distinguer ce qui relève du faisable, du souhaitable et de l'irresponsable, afin de construire des décisions solides, assumables et durables.

PARTIE 1 : LA RATIONALITÉ DE LA VIDÉOPROTECTION

LECTURE RAPIDE : DE LA RATIONALITÉ DANS LE DÉBAT SUR LA VIDÉOPROTECTION

LA PREMIÈRE PARTIE DE CE LIVRE BLANC VISE À POSER LES BASES D'UN DÉBAT LUCIDE ET RESPONSABLE SUR LA VIDÉOPROTECTION À L'ÉCHELLE DU MANDAT MUNICIPAL 2026-2032. ELLE S'ADRESSE EN PRIORITÉ AUX MAIRES ET AUX ÉQUIPES QUI SOUHAITENT COMPRENDRE CE QUI RELÈVE RÉELLEMENT DE LEUR RESPONSABILITÉ, CE QUI PEUT ÊTRE ATTENDU D'UN DISPOSITIF DE VIDÉOPROTECTION, ET DANS QUEL CADRE JURIDIQUE ET POLITIQUE CES DÉCISIONS DOIVENT ÊTRE PRISES.

Le chapitre 1 part du point de vue du maire. Il rappelle que la sécurité et la tranquillité publique constituent une attente forte des habitants, mais que cette attente est souvent marquée par des confusions entre ce qui relève de la commune, de l'État, de la prévention ou de la justice. Ce chapitre aide à clarifier les responsabilités réelles du maire, à distinguer ce que les habitants attendent vraiment de ce qu'ils projettent symboliquement, et à comprendre pourquoi la vidéoprotection devient un sujet électoral récurrent, y compris lorsqu'elle n'est pas, à elle seule, une solution.

Le chapitre 2 s'attache à clarifier ce qu'est réellement la vidéoprotection aujourd'hui. Il met fin aux confusions fréquentes entre vidéosurveillance, vidéoprotection, centres de supervision et usages associés. Il rappelle surtout à quoi sert une caméra, et à quoi elle ne sert jamais. Ce chapitre insiste sur un point central : la vidéoprotection est un outil d'observation et d'appui, utile dans certains contextes précis, mais qui ne remplace ni la présence humaine, ni la prévention, ni l'action judiciaire. Il invite les élus à sortir des promesses implicites irréalistes pour adopter un positionnement plus robuste et défendable.

Le chapitre 3 propose une lecture claire du cadre juridique et institutionnel à connaître avant toute décision. Sans entrer dans un excès de technicité, il explique comment s'articulent les responsabilités entre le maire, le préfet et les services de l'État, et pourquoi cette articulation est déterminante pour la solidité des projets. Il met également en lumière les différences de règles selon les espaces concernés, espace public, bâtiments municipaux, espaces privés ouverts au public, distinctions souvent sous-estimées mais essentielles pour éviter les erreurs de conception.

Le chapitre 4 aborde frontalement les trois critiques les plus fréquemment formulées à l'encontre
de la vidéoprotection : son coût, son impact sur les libertés publiques et son efficacité réelle. Plutôt que de les balayer ou feindre de les ignorer, ce chapitre propose des réponses argumentées, fondées sur des réalités budgétaires, juridiques et opérationnelles. Il permet aux élus de se doter d'éléments de langage solides, sans tomber dans une posture défensive ou idéologique.

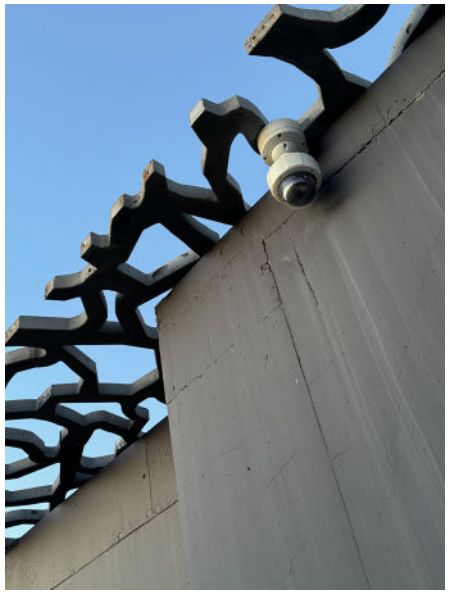
Le chapitre 5 marque un tournant plus stratégique. Il ne s'agit plus seulement de comprendre, mais de poser des principes de décision. Ce chapitre explique pourquoi une vidéoprotection utile ne se mesure ni au nombre de caméras ni à des standards abstraits, mais à la manière dont les usages sont ciblés, proportionnés et assumés politiquement. Il fournit une grille de lecture permettant de distinguer un projet défendable d'un projet fragile, indépendamment de la taille de la collectivité.

Enfin, **le chapitre 6 élargit la réflexion aux nouvelles menaces et aux évolution**s du contexte, qu'il s'agisse des risques liés aux événements de masse, à l'usage de drones, aux enjeux de cybersécurité ou aux nouvelles obligations réglementaires. Il aide les élus à comprendre ce qu'il est pertinent d'anticiper dès aujourd'hui, sans nécessairement s'équiper immédiatement, et ce qu'il serait imprudent de promettre dans un programme municipal.

DANS SON ENSEMBLE, CETTE PREMIÈRE PARTIE VISE À DONNER AUX ÉLUS LES REPÈRES NÉCESSAIRES POUR SORTIR D'UN DÉBAT CARICATURAL, REPRENDRE LA MAIN SUR LE RÉCIT PUBLIC ET ABORDER LA VIDÉOPROTECTION NON COMME UN SYMBOLE, MAIS COMME UN OUTIL PARMI D'AUTRES, À INTÉGRER DANS UNE STRATÉGIE DE MANDAT COHÉRENTE, PROGRESSIVE ET ASSUMÉE.

1.LE MANDAT 2026–2032 VU D'UN MAIRE

1.1. Les responsabilités réelles du maire en matière de sécurité et de tranquillité publique



Un maire n'est ni un chef de la police nationale, ni un procureur, mais il n'est pas non plus un spectateur impuissant de sa commune. La loi lui confie une responsabilité claire et directe en matière de tranquillité publique, de prévention des troubles à l'ordre public et de protection des personnes et des biens sur le territoire communal. Cette responsabilité est politique, juridique et opérationnelle. Elle s'exerce au quotidien, dans l'espace public, dans les équipements municipaux, dans l'organisation des services, et dans la capacité à anticiper des situations dégradées avant qu'elles ne deviennent des crises.

Ce cadre est souvent volontairement brouillé dans le débat public. Certains laissent entendre que la sécurité relèverait exclusivement de l'État, d'autres promettent aux habitants une capacité d'action locale illimitée. Les deux discours sont faux. Le maire agit dans un champ précis, encadré par le Code de la sécurité intérieure, avec des leviers concrets comme la police municipale, la vidéoprotection, l'éclairage public, l'aménagement urbain, la gestion des événements et la coordination avec les services de l'État. Ne pas agir dans ce champ, ou agir de manière désordonnée, engage sa responsabilité.

La vidéoprotection s'inscrit dans ce périmètre. Elle n'est ni une compétence régalienne détournée, ni une dérive autoritaire par nature. Elle est un outil mis à disposition des communes pour les aider à remplir une mission légale, sous contrôle préfectoral et dans un cadre juridique strict. La question n'est donc pas de savoir si un maire a le droit d'y recourir, mais s'il sait pourquoi, comment et dans quelles limites il le fait.

1.2. Ce que les habitants attendent vraiment, et ce qu'ils confondent

Les habitants ne demandent pas des caméras. Ils demandent à être protégés, en temps réel. Cette nuance est centrale et trop souvent ignorée. Lorsqu'un citoyen parle de sécurité, il ne raisonne pas en architecture de systèmes, en articles de loi ou en débats idéologiques. Il parle de situations concrètes, ici et maintenant. Une agression évitée, une intervention plus rapide, un malaise détecté à temps, un incendie repéré avant qu'il ne se propage. Ce qu'il attend, c'est une capacité de réaction, pas uniquement une promesse d'élucidation a posteriori.

Or une grande partie du débat public confond deux temporalités radicalement différentes. D'un côté, la protection en temps réel, qui vise à détecter une situation anormale et à permettre une intervention immédiate. De l'autre, la vidéo-élucidation, qui intervient après les faits, quand le dommage est déjà là. Les habitants perçoivent très bien cette différence, même s'ils ne la formulent pas ainsi. Ils savent intuitivement que retrouver un auteur plusieurs jours plus tard ne répare ni le traumatisme, ni les conséquences subies.

C'est précisément là que la vidéoprotection prend tout son sens lorsqu'elle est couplée à des opérateurs formés et, le cas échéant, à des outils de Remontée Automatique d'Alerte (R2A, Cf. Partie n°2 de ce document). Non pas pour surveiller en permanence, mais pour signaler plus vite ce qui mérite une attention humaine, une lever de doute. L'algorithme ne décide pas, il alerte. L'opérateur ne condamne pas, il évalue et alerte le bon service. Et l'élu n'abdique pas devant sa responsabilité, il organise une capacité d'action cohérente avec les attentes de sa population.

1.3. Pourquoi la vidéoprotection devient un sujet électoral récurrent, même quand elle n'est pas la solution

Si la vidéoprotection revient systématiquement dans les campagnes municipales, ce n'est pas parce qu'elle serait une solution universelle, mais parce qu'elle est un symbole politique puissant. Visible, matérialisable, facilement compréhensible, elle donne l'illusion d'une action immédiate sur un sujet anxiogène. À l'inverse, expliquer ce que l'on ne peut pas faire, ce qui relève de l'État, ou ce qui prendra plusieurs années est électoralement moins confortable.

Cette récurrence est entretenue par deux excès opposés. D'un côté, des promesses maximalistes qui laissent croire qu'un déploiement de caméras réglerait à lui seul les problèmes de sécurité. De l'autre, une opposition idéologique qui présente toute forme de vidéoprotection comme une dérive liberticide ou une surveillance de masse déguisée. Ces deux positions évitent soigneusement la réalité opérationnelle, juridique et budgétaire des communes.

En pratique, la vidéoprotection n'est ni une panacée ni un danger systémique. Elle est parfois pertinente, parfois inutile, parfois contre-productive si elle est mal pensée. La responsabilité politique du maire consiste précisément à sortir de ce faux dilemme. Dire où la caméra a un intérêt réel, où elle n'en a aucun, et surtout ce qu'elle ne remplacera jamais. Ce positionnement lucide est plus difficile à tenir en campagne, mais c'est le seul qui permette de construire une stratégie crédible sur la durée d'un mandat.

2. CE QU'EST RÉELLEMENT LA VIDÉOPROTECTION AUJOURD'HUI

La vidéoprotection souffre d'un mal structurel dans le débat public depuis 20 ans : tout le monde en parle, très peu savent précisément de quoi ils parlent. Les termes sont employés de manière interchangeable, volontairement ou par ignorance, ce qui nourrit à la fois les peurs infondées et les promesses irréalistes. Avant de débattre de son utilité, de ses limites ou de son évolution vers la R2A (Remontée d'Alerte Automatique), il est indispensable de remettre des définitions claires sur des réalités très différentes. Ce travail n'est pas théorique. Il conditionne la pertinence des choix politiques et la crédibilité du discours tenu aux habitants.

2.1. Vidéosurveillance, vidéoprotection, CSU, CSUi, CSD : mettre fin aux confusions

La première confusion est sémantique mais elle est lourde de conséquences. En droit français, le terme de vidéoprotection désigne un dispositif encadré par le Code de la sécurité intérieure, autorisé par le préfet, limité à des finalités précises (11 au sein du L251-2) et placé sous la responsabilité du maire lorsqu'il s'agit de l'espace public communal (une rue publique de la commune) ou des espaces privés ouverts au public (la galerie d'un centre commercial, une pharmacie, un buraliste). La vidéosurveillance, au sens juridique, relève quant à elle des espaces privés (une usine, un site sensible…). Employer l'un pour l'autre n'est pas neutre, car cela revient à mélanger des régimes juridiques, des responsabilités et des contrôles qui n'ont rien à voir.

La deuxième confusion porte sur les centres de supervision. Un CSU (Centre de Supervision Urbain) n'est pas une salle d'écrans spectaculaire, ni un symbole de pouvoir. C'est un outil organisationnel, au service d'opérateurs humains, chargés d'exploiter des images dans un cadre précis et selon des procédures définies. Dans la majorité des communes françaises, la taille critique pour faire fonctionner un CSU en continu n'est tout simplement pas atteinte. Vouloir un CSU communal h24 sans opérateurs dédiés est parfois une obligation, le CSU est alors utilisé en relecture à des fins d'élucidation. C'est là qu'intervient naturellement la notion de mutualisation. Le CSUi, à l'échelle intercommunale, ou le CSD, centre de supervision départemental lorsqu'un département s'est doté d'un tel dispositif, constituent aujourd'hui des réponses réalistes aux contraintes humaines et organisationnelles rencontrées par la majorité des communes. Le cadre juridique autorise explicitement ces organisations mutualisées, notamment via des syndicats mixtes numériques portés par les départements, conformément aux dispositions issues de la loi de sécurité globale préservant les libertés de 2021.

Cette approche n'est pas une obligation uniforme ni une remise en cause des choix locaux. Elle s'inscrit dans une tendance de fond observée à l'échelle nationale, liée à la recherche de continuité de

service, de professionnalisation des opérateurs et de capacité de réaction en temps réel. Du point de vue de l'AN2V, c'est à cette échelle que se joue, pour de nombreuses collectivités, le passage progressif d'une logique principalement orientée vers la vidéo-élucidation à une vidéoprotection réellement tournée vers la protection immédiate des personnes et des biens.

2.2. À quoi sert une caméra, et à quoi elle ne sert jamais

Une caméra ne pense pas, ne décide pas et ne protège personne par elle-même. Elle capte des images. Tout le reste relève des usages qui en sont faits, de l'organisation humaine qui les encadre et des finalités politiques qui leur sont assignées. Considérée comme un capteur, la caméra peut contribuer à des objectifs différents selon le contexte : protection des personnes et des biens, observation des dynamiques de la commune, aide à la décision publique ou analyse a posteriori de situations complexes. Lorsqu'elle est intégrée dans un dispositif cohérent, avec des opérateurs formés, des procédures claires et une chaîne décisionnelle maîtrisée, la caméra peut contribuer à détecter plus tôt une situation anormale et à déclencher une intervention plus rapide. C'est le cas notamment pour des usages liés à la sécurité, à la gestion d'événements, au secours aux personnes ou à la prévention de risques immédiats. Dans ces configurations, la valeur de la caméra tient moins à l'image elle-même qu'à la capacité de l'organisation à transformer une information visuelle en action adaptée.



Mais la caméra n'est pas réservée aux seuls usages sécuritaires. Elle constitue également un outil d'observation et de mesure des usages de l'espace public. Elle peut permettre de compter des flux piétons, trottinettes ou automobiles, d'analyser l'utilisation réelle d'un aménagement, d'objectiver des phénomènes de congestion, d'évaluer l'impact d'une modification de la signalisation ou de suivre l'évolution d'un risque naturel comme une montée des eaux ou un débordement localisé. Dans ces cas, il ne s'agit pas de vidéoprotéger des individus, mais de comprendre des situations, sur la durée, afin d'ajuster des politiques publiques en matière de mobilités, d'urbanisme, de transition écologique ou de résilience territoriale.

Une caméra ne supprime ni la délinquance, ni les trafics de stupéfiants, ni les conflits sociaux, ni les violences intrafamiliales, ni les formes de délinquance diffuse. Elle n'agit ni sur les causes profondes ni sur les logiques sociales ou économiques qui les sous-tendent. Elle ne remplace ni la présence humaine sur le terrain, ni les actions de prévention, ni le travail d'enquête et de justice, et ne peut être présentée comme une réponse globale à des problématiques complexes.

En revanche, la vidéoprotection peut, dans certains contextes précis, contribuer à objectiver des situations, à documenter des usages de l'espace public, à sécuriser des abords ou à appuyer une action coordonnée avec les forces de sécurité compétentes. Lui attribuer un rôle qu'elle ne peut pas tenir procède d'une simplification excessive du débat public et crée des attentes irréalistes. C'est ce décalage entre ce que la caméra peut réellement apporter et ce qu'on lui fait symboliquement porter qui alimente les critiques les plus virulentes et fragilise les projets mal cadrés.

Il convient également de distinguer les usages selon l'organisation dont dispose la collectivité et selon la temporalité de l'action. Lorsqu'un opérateur est présent et en capacité de traiter des images en continu h24 et 365j/an, notamment sur des plages horaires qui s'avèrent critiques, la caméra peut contribuer à une action en temps réel, orientée vers la protection immédiate des personnes et des biens. Mais dans de nombreuses communes, en particulier les plus petites, l'absence d'opérateur dédié rend cet usage impossible, sans pour autant priver le dispositif de toute pertinence.

Dans ces configurations, la caméra demeure un outil particulièrement efficace de consultation a posteriori et d'analyse différée. Elle permet d'élucider plus rapidement des faits, à charge comme à décharge, d'appuyer le travail des forces de sécurité, de prévenir les récidives par un effet dissuasif connu, mais aussi d'analyser des usages, d'évaluer des aménagements ou de documenter des phénomènes de la collectivité sur la durée. Ces usages différés, qu'ils relèvent de la sécurité ou de la gestion urbaine, sont pleinement légitimes, à condition de ne pas être présentés comme équivalents à une capacité de protection en temps réel.

2.3. La vidéoprotection comme outil parmi d'autres, pas comme réponse globale

La vidéoprotection n'est ni une politique de sécurité en soi, ni une fin en soi. Elle est un composant parmi d'autres d'un écosystème plus large, qui inclut la présence humaine, l'aménagement de l'espace public, la prévention, la coordination avec les forces de l'État et la capacité à gérer des situations exceptionnelles. La réduire à un débat pour ou contre est une impasse intellectuelle et politique.

C'est également dans ce cadre qu'il faut comprendre l'apport potentiel de la Remontée Automatique d'Alerte.



La R2A n'est pas une surcouche magique, ni un substitut à l'humain. Elle n'a de sens que si une organisation existe pour recevoir, qualifier et traiter les alertes. Pour les communes de petite taille, cela implique mécaniquement une réflexion à une échelle supérieure : intercommunale ou départementale.
Un maire responsable ne promet pas une technologie. Il construit une capacité. Cela suppose de choisir les bons outils, à la bonne échelle, pour les bons usages, et d'assumer clairement ce que l'on fait, ce que l'on ne fait pas et ce que l'on ne fera jamais. C'est cette lucidité qui permet de sortir durablement des fantasmes, qu'ils soient technophiles ou technophobes.

3. LE CADRE JURIDIQUE ET INSTITUTIONNEL À CONNAÎTRE AVANT DE DÉCIDER

La vidéoprotection n'est ni une zone grise juridique, ni un champ d'expérimentation libre laissé à l'appréciation des communes. Elle repose sur un cadre légal précis, ancien (Loi de 1995), consolidé au fil des années, et contrôlé à plusieurs niveaux. Pour un élu local, il n'est pas nécessaire d'en maîtriser tous les détails techniques, mais il est indispensable d'en comprendre la logique générale, les responsabilités respectives des acteurs et les conséquences concrètes de chaque choix d'implantation ou d'usage.

Ce cadre a une vertu souvent sous-estimée dans le débat public. Il protège à la fois les libertés individuelles et les décideurs locaux. Lorsqu'un projet est conçu dans le respect du droit, il devient politiquement défendable, juridiquement sécurisé et opérationnellement utile. À l'inverse, l'approximation ou la méconnaissance exposent inutilement les élus à des critiques, des recours et parfois à des blocages.

3.1. Le Code de la sécurité intérieure et les 11 finalités de l'article L251-2

Le socle juridique de la vidéoprotection sur la voie publique repose sur le Code de la sécurité intérieure, et plus précisément sur les 11 finalités d'usages décrits dans l'article L251-2. Cet article encadre de manière précise et limitative dans l'espace et le temps les conditions dans lesquelles un système de vidéoprotection peut être autorisé par le préfet.
La vidéoprotection peut ainsi être autorisée pour les finalités suivantes : 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 exposés à des risques particuliers, la prévention d'actes de terrorisme, la prévention des risques naturels ou technologiques, le secours aux personnes, la lutte contre l'incendie, la protection des abords des sites sensibles et, plus largement, la prévention des atteintes graves à l'ordre public.
Ces finalités ne sont pas de simples formules administratives. Elles conditionnent l'autorisation préfectorale, le positionnement des caméras, leur orientation, les modalités d'exploitation des images, leur durée d'enregistrement (maximum 30 jours) et les usages possibles de la R2A. Toute utilisation qui ne se rattache pas clairement à l'une de ces finalités est juridiquement fragile, voire illégale.

3.2. Qui fait quoi : maire, préfet, référent sûreté, forces de sécurité intérieure

Lorsqu'un projet de vidéoprotection concerne l'espace public communal, le maire en est l'initiateur. Il en assume la responsabilité politique et opérationnelle, dans le cadre des pouvoirs de police administrative qui lui sont confiés par la loi. À ce titre, il décide d'engager ou non un projet, d'en définir les objectifs et d'en assurer la cohérence avec les besoins du territoire.
Le préfet joue un rôle central dans ce dispositif. Il autorise l'installation après examen du dossier par la CDV (Commission Départementale de Vidéoprotection), contrôle la conformité du projet aux finalités légales, fixe les conditions d'exploitation des systèmes et peut retirer l'autorisation en cas de manquement. Cette intervention de l'État ne constitue pas une contrainte formelle, mais un mécanisme de sécurisation juridique pour les élus locaux, garantissant que le dispositif s'inscrit dans un cadre partagé et validé au niveau national.

Les forces de sécurité intérieure interviennent en articulation avec les dispositifs communaux, sans en être les opérateurs systématiques. Elles peuvent accéder aux images dans des conditions strictement encadrées, notamment dans le cadre d'enquêtes ou de réquisitions judiciaires. Les référents sûreté, rattachés à la police nationale ou à la gendarmerie nationale, jouent quant à eux un rôle de conseil en amont des projets. Ils accompagnent les collectivités pour cibler les besoins réels, éviter les erreurs de conception et contribuer à l'instruction des dossiers présentés en Commission Départementale de Vidéoprotection en vue de la décision préfectorale.

3.3. Espaces publics, bâtiments municipaux, espaces privés ouverts au public : ce que cela change concrètement

Le régime juridique de la vidéo varie fortement selon la nature des espaces concernés. Sur les espaces publics et les espace privés ouverts au public, le cadre est le plus strict. Toute installation est soumise à autorisation préfectorale, à des obligations d'information du public, à des durées de conservation limitées et à des contrôles réguliers. C'est sur cet espace que se concentrent l'essentiel des débats et des fantasmes.
Dans les bâtiments municipaux, le cadre peut différer selon qu'ils sont ouverts ou non au public, et selon les finalités poursuivies. Les obligations restent importantes, mais les marges de manœuvre sont parfois plus larges, notamment pour des enjeux de protection des agents, des équipements ou des usagers.
Comprendre ces distinctions est essentiel pour éviter les erreurs de périmètre, les attentes irréalistes et les critiques infondées. Un projet juridiquement solide commence toujours par une lecture fine des espaces concernés et des responsabilités associées.

4. TROIS CRITIQUES, TROIS RÉPONSES : CHER, LIBERTICIDE, INEFFICACE

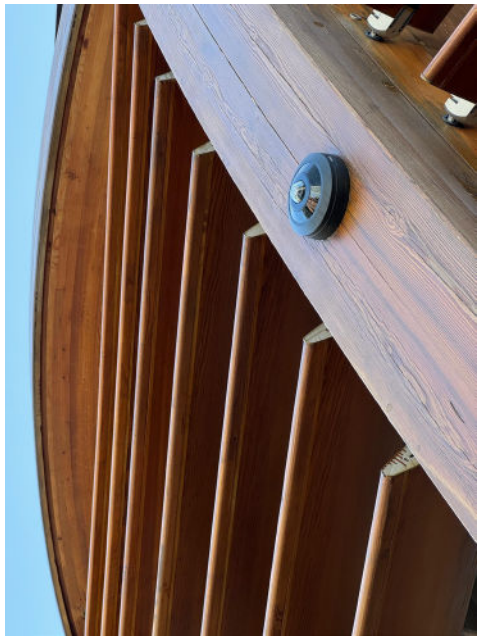
Depuis plus de vingt ans, la vidéoprotection fait l'objet de critiques récurrentes, qui ressurgissent à chaque projet local et à chaque échéance électorale. Trois arguments reviennent systématiquement : son coût jugé excessif, son caractère supposé liberticide et son inefficacité présumée. Ces critiques ne doivent ni être balayées d'un revers de main, ni être acceptées comme des évidences. Elles méritent au contraire d'être examinées, à la lumière des faits, des usages réels et des cadres juridiques existants.

4.1. « C'est cher » - coût réel, coût évité, mutualisation, arbitrage avec d'autres dépenses

Dire qu'un dispositif est « cher » n'a de sens que si l'on précise par rapport à quoi. En valeur absolue, un système de vidéoprotection représente effectivement un investissement pour une commune, auquel s'ajoutent des coûts de fonctionnement liés à la maintenance, aux réparations et à l'exploitation du dispositif (les opérateurs vidéo). En valeur relative, rapportée aux budgets publics consacrés à la sécurité, à la prévention ou à la réparation des dommages, cette appréciation mérite toutefois d'être nuancée. À l'échelle nationale, les dépenses annuelles liées à la vidéoprotection représentent une part marginale des budgets de sécurité, très inférieure à d'autres postes structurels, comme la masse salariale du ministère de l'Intérieur ou, à l'échelle locale, le coût cumulé d'une police municipale sur la durée d'un mandat.
Apprécié sur l'ensemble d'un mandat, le coût global d'un dispositif de vidéoprotection, en investissement et en fonctionnement, représente généralement une fraction limitée du budget consacré à la sécurité et à la tranquillité publique. Dans ce cadre, la vidéoprotection ne doit pas être envisagée comme une dépense isolée, mais comme un outil parmi d'autres contribuant au fonctionnement global de la collectivité, au même titre que les moyens humains ou les équipements urbains.
Surtout, un raisonnement strictement comptable occulte la notion de coût évité. Une intervention plus rapide, un fait élucidé sans mobilisation prolongée de moyens humains, une enquête orientée plus efficacement ou une récidive empêchée ont un impact économique réel, bien que difficile à mesurer de manière directe dans les budgets locaux. Ces effets, rarement visibles ligne par ligne, n'en sont pas moins déterminants pour l'efficience globale de l'action publique.

Enfin, le coût de la vidéoprotection dépend largement de l'organisation retenue. La mutualisation, qu'elle soit intercommunale ou départementale, peut permettre de lisser les dépenses, de professionnaliser l'exploitation et d'éviter la multiplication de dispositifs sous-utilisés. Le véritable enjeu n'est donc pas le prix unitaire des équipements, mais la cohérence du projet, son dimensionnement, son intégration et son articulation avec les autres politiques publiques locales.

4.2. « C'est liberticide » - ce qui est interdit, ce qui est encadré, ce qui est maîtrisable localement



La crainte d'une atteinte aux libertés publiques est légitime dans une démocratie. Elle devient problématique lorsqu'elle repose sur une vision théorique ou fantasmée de la vidéoprotection, déconnectée de son cadre juridique réel. En France, la vidéoprotection sur la voie publique est strictement encadrée par la loi, autorisée par le préfet, contrôlée par la CNIL et limitée à des finalités précises. Elle ne permet ni une surveillance généralisée, ni une exploitation libre des images.
Contrairement à certaines représentations, la très grande majorité de l'espace public n'est pas couverte par des caméras, même dans les grandes villes. Les dispositifs sont ciblés, localisés et visibles. Les durées de conservation sont limitées (maximum 30 jours), l'accès aux images est tracé et toute utilisation abusive est sanctionnable. De plus, tant qu'une image n'est pas visionnée par un opérateur habilité ou exploitée dans un cadre judiciaire, elle n'a aucun effet concret sur les libertés individuelles.
Il est également utile de rappeler que la société contemporaine est déjà traversée par une production massive d'images, issues notamment des smartphones, des réseaux sociaux et des dispositifs privés, sur lesquels les collectivités n'ont aucun contrôle. La spécificité de la vidéoprotection publique réside précisément dans son encadrement démocratique et institutionnel. Le débat sur les libertés ne porte donc pas sur l'existence des images, mais sur leur gouvernance, leur transparence et les limites que la collectivité se fixe.

4.3. « C'est inefficace » - ce que montrent les retours d'expérience, où la caméra ne sert à rien, où elle change vraiment la donne

L'inefficacité supposée de la vidéoprotection est souvent évaluée à l'aune d'un critère unique : la baisse globale de la délinquance. Or aucun outil, technologique ou humain, ne peut à lui seul produire un tel effet. La vidéoprotection n'a jamais eu vocation à éradiquer la délinquance. Elle agit à trois niveaux distincts : avant, pendant et après les faits.
Avant les faits, elle peut jouer un rôle dissuasif ou de prévention situationnelle dans certains contextes précis, en rendant le passage à l'acte plus risqué ou plus visible. Pendant les faits, lorsqu'elle est couplée à une organisation adaptée, elle permet de détecter des situations anormales et de déclencher des interventions plus rapides et mieux ciblées, surtout avec la R2A de la partie n°2 de ce document. Après les faits, elle constitue un outil précieux pour l'élucidation rapide des situations, l'orientation des enquêtes à partir d'éléments factuels et concordants, ainsi que pour la prévention des récidives.
À l'inverse, les situations dans lesquelles la vidéoprotection est inefficace sont bien identifiées : absence d'opérateur aux périodes cruciales, implantation mal pensée, objectifs flous ou attentes irréalistes. Reconnaître ces limites n'est pas un aveu d'échec, mais une condition de crédibilité.

4.4. Comment sortir du faux débat «pour ou contre les caméras» pour passer au «pour quoi faire, où, et comment» ?

Le débat public se focalise trop souvent sur une opposition binaire entre partisans et opposants à la vidéoprotection. Cette grille de lecture simplificatrice masque les véritables enjeux et empêche toute décision rationnelle à l'échelle locale. Elle réduit un outil à un symbole, alors même que ses usages, ses limites et ses effets dépendent entièrement des choix politiques qui l'encadrent.
La question pertinente pour une collectivité n'est donc pas d'adhérer ou de s'opposer par principe à la caméra, mais de définir clairement ce qu'elle cherche à faire, sur quels périmètres, avec quelle organisation et dans quelles limites. Ce déplacement du débat permet d'aborder de manière apaisée la diversité des usages possibles, les contraintes juridiques associées et les arbitrages nécessaires entre protection, gestion des espaces publics et acceptabilité sociale.
Un projet de vidéoprotection n'est légitime et pertinent que s'il répond à un besoin identifié, s'il s'inscrit dans un cadre juridique maîtrisé et s'il est compréhensible pour les habitants parce qu'il est expliqué, débattu et évalué. Sortir des postures idéologiques, qu'elles soient technophiles ou technophobes, est la condition indispensable pour construire des décisions locales responsables, ajustables dans le temps et durablement acceptées.

TEMPS RÉEL OU TEMPS DIFFÉRÉ ?

Attente citoyenne	Temps réel
Être protégé immédiatement	Surveillance continue
Qu'une intervention soit déclenchée	Détection -> levée de doute -> Alerte
Éviter que la situation dégénère	Minutes gagnées sur l'intervention

Le temps réel n'existe que s'il y a des opérateurs.

Bénéfices collectifs	Temps différé
Élucidation des faits	Relecture et extraction d'images
Appui aux enquêtes	Éléments probants
Analyse & prévention	Analyse et aide à la décision

Le temps différé ne répond pas à l'urgence, il répond à la responsabilité publique.

Promettre du "temps réel" sans moyens humains crée une attente citoyenne impossible à tenir.

5. VIDÉOPROTECTION UTILE : PRINCIPES, LIGNES ROUGES ET RESPONSABILITÉS POLITIQUES

La vidéoprotection n'est ni neutre, ni automatique, ni anodine. Elle engage des choix politiques explicites, qui doivent être assumés, expliqués et encadrés dans la durée. Une commune responsable ne se définit pas par le nombre de caméras installées, ni par le nombre de caméra par habitants, mais par la manière dont elle articule les besoins fonctionnels du territoire, les attentes des habitants, les difficultés potentielle locale, le cadre juridique et les moyens réellement disponibles. À ce titre, la question centrale n'est pas celle de la capacité technologique, mais celle de la légitimité des usages.
Ce chapitre vise à poser des principes clairs, applicables à toutes les tailles de collectivités, quels que soient leurs choix d'équipement. Il ne s'agit pas d'un catalogue de bonnes intentions, mais d'une grille de lecture opérationnelle permettant de distinguer un projet défendable d'un projet fragile, tant juridiquement que politiquement.

5.1. Proportionnalité, ciblage, temporalité : les trois filtres d'un projet défendable

Un projet de vidéoprotection défendable ne se juge pas uniquement à l'aune des enjeux de sécurité ou de délinquance. Il doit être proportionné aux usages poursuivis, qu'ils relèvent de la tranquillité publique, de la gestion des mobilités, de la transition écologique, de la prévention des risques ou de l'optimisation des services urbains. La proportionnalité consiste à adapter le dispositif non seulement aux risques identifiés, mais aussi aux bénéfices attendus pour le fonctionnement global du territoire. Une caméra destinée à sécuriser un carrefour accidentogène, à mesurer l'usage réel d'une piste cyclable ou à surveiller un point sensible en cas de crue ne répond pas aux mêmes logiques, mais doit être soumise au même niveau d'exigence politique et juridique.
Le ciblage constitue le deuxième filtre structurant. Une vidéoprotection utile est toujours déployée pour répondre à des situations concrètes et observables. Elle peut concerner des lieux exposés à des faits de délinquance, mais aussi des axes de circulation saturés, des carrefours mal régulés, des zones de forte fréquentation piétonne, des voies douces nouvellement créées ou des secteurs soumis à des risques naturels récurrents. Le ciblage permet de sortir d'une logique de surveillance diffuse pour entrer dans une logique d'outil d'aide à la décision publique, fondée sur l'observation, la mesure et l'évaluation des politiques locales.
Enfin, la temporalité est un critère déterminant, trop souvent réduit à la seule question du temps réel. Un dispositif de vidéoprotection peut produire de la valeur à différentes échelles de temps. En temps réel, lorsqu'une organisation le permet, il contribue à la protection des personnes et des biens. En temps différé, il permet d'analyser les usages d'un espace public, d'évaluer l'efficacité d'un aménagement, d'objectiver des choix de circulation ou de documenter l'évolution d'un phénomène urbain. Accepter cette pluralité des temporalités, c'est reconnaître que la vidéoprotection n'est pas uniquement un outil de réaction, mais aussi un instrument d'aide à la compréhension et à l'ajustement des politiques publiques locales.

5.2. Transparence, information du public, rôle du conseil municipal

La légitimité d'un dispositif de vidéoprotection repose autant sur ses usages que sur la manière dont il est gouverné et expliqué. La transparence n'est pas une obligation formelle à satisfaire a minima, mais un levier politique essentiel pour construire la confiance et éviter les incompréhensions durables. Informer le public ne consiste pas seulement à apposer des panneaux réglementaires, mais à rendre lisible le sens du projet, ses objectifs, ses limites et les garanties qui l'encadrent.
Cette exigence de transparence vaut quel que soit l'usage poursuivi, qu'il s'agisse de sécurité, de gestion des mobilités, de prévention des risques ou d'observation des usages urbains. Les habitants acceptent d'autant mieux un dispositif qu'ils comprennent à quoi il sert, ce qu'il ne permet pas et dans quel cadre il est contrôlé. À l'inverse, l'opacité ou le flou nourrissent les soupçons, même lorsque les usages sont parfaitement légaux et proportionnés.
Le conseil municipal joue à ce titre un rôle central. Il ne peut être réduit à une simple validation technique ou administrative. Débattre en conseil des objectifs poursuivis, des périmètres concernés, des principes de gouvernance et des modalités d'évaluation permet d'ancrer le projet dans une décision collective assumée. Cette mise en débat protège les élus, renforce la solidité juridique du dispositif et évite que la vidéoprotection ne soit perçue comme un projet imposé ou technocratique.
Enfin, une information régulière et factuelle, fondée sur des éléments objectivables et des retours d'expérience, permet d'inscrire le dispositif dans le temps long du mandat. Expliquer ce qui fonctionne, ce qui a été ajusté, ce qui a été abandonné contribue à normaliser l'usage de la vidéoprotection comme un outil de politique publique parmi d'autres, soumis à l'évaluation et à l'amélioration continue. On pourra utilement mettre en place un comité d'Éthique (Cf. chapitre 16) qui se réunit régulièrement, et dont les comptes-rendus sont portés au bulletin municipal.



5.3. Ce qu'une commune responsable s'interdit, même si la technologie le permet

La responsabilité politique d'une commune ne se mesure pas uniquement à ce qu'elle met en œuvre, mais aussi à ce qu'elle choisit délibérément de ne pas faire. Les capacités technologiques évoluent plus vite que le droit et que l'acceptabilité sociale. Une collectivité responsable se fixe donc des lignes rouges internes claires, indépendamment de ce que les outils pourraient techniquement permettre.
Elle s'interdit en premier lieu tout usage sans base légale explicite ou sans rattachement clair aux finalités prévues par le Code de la sécurité intérieure ou la CNIL. Elle refuse les détournements de finalité, les extensions implicites de périmètre ou les usages opportunistes qui fragiliseraient juridiquement et politiquement le dispositif. Cette rigueur est indispensable pour préserver la crédibilité de l'action publique et éviter les contentieux.
Une commune responsable s'interdit également de déléguer des choix politiques à des solutions techniques ou à des prestataires. Les outils d'automatisation, lorsqu'ils existent, ne doivent jamais devenir des décideurs : Ils peuvent assister l'analyse humaine, alerter, prioriser ou objectiver, mais la décision finale reste humaine, contextualisée et assumée. Toute automatisation sans gouvernance claire, sans procédures et sans contrôle expose la collectivité à des risques éthiques, juridiques et réputationnels.
Enfin, une commune responsable s'interdit de promettre ce qu'elle ne peut pas tenir. Elle ne présente pas la vidéoprotection comme une réponse globale à des problématiques complexes, ni comme un substitut à la présence humaine, à la prévention ou à l'action judiciaire. Elle assume clairement les limites du dispositif, qu'il s'agisse de l'absence d'opérateur en temps réel, de contraintes budgétaires ou de choix organisationnels. Cette honnêteté est la condition pour construire une acceptabilité durable et éviter les désillusions en cours de mandat.

5.4. Lancer un projet de vidéoprotection : les choix structurants que le maire ne doit pas déléguer

Le succès ou l'échec d'un projet de vidéoprotection se joue largement avant la première caméra installée. Les erreurs commises au démarrage sont rarement visibles immédiatement, mais elles conditionnent durablement l'efficacité, les coûts et l'évolutivité du dispositif sur l'ensemble du mandat.
La première vigilance consiste à raisonner en besoins opérationnels et non en solutions techniques.

Le rôle de l'élu n'est pas de choisir un modèle de caméra ou une architecture réseau, mais d'exprimer clairement ce qui doit être observé ou compris : un flux de véhicules, une zone de conflit d'usages, une entrée de ville, un site sensible. C'est à l'intégrateur, sous le contrôle de la collectivité, de proposer les technologies, les emplacements et les infrastructures adaptées. Inverser cette logique conduit presque toujours à des dispositifs inadaptés ou surdimensionnés.
Dès l'amont, le projet doit être piloté de manière transversale. Le cantonner à la seule police municipale est une erreur fréquente. Les directions des services techniques et des systèmes d'information doivent être associées dès la conception, car les enjeux de réseaux, d'alimentation, de cybersécurité et de maintenance conditionnent directement la pérennité du système. Un projet techniquement performant mais mal intégré au fonctionnement de la collectivité devient rapidement une charge plutôt qu'un outil.
Certains choix techniques relèvent toutefois de décisions stratégiques. Pour des usages spécifiques, notamment la surveillance nocturne ou les entrées de ville, toutes les caméras ne se valent pas. Des équipements dédiés, par exemple pour la lecture de plaques d'immatriculation, peuvent s'avérer indispensables, là où des caméras standards seraient inefficaces. De même, en l'absence d'un opérateur présent en continu, privilégier des caméras fixes et bien positionnées est souvent plus pertinent que des dispositifs motorisés sous-exploités.
La question de l'évolutivité est également centrale. Le choix de systèmes ouverts et non propriétaires permet d'éviter l'enfermement technologique, de maîtriser les coûts à moyen terme et d'intégrer plus tard de nouveaux équipements ou logiciels sans remettre en cause l'ensemble du dispositif.
Sur le plan financier, le maire doit être particulièrement attentif au coût réel du système sur la durée du mandat. Le prix d'achat initial est rarement représentatif de l'effort budgétaire global : Abonnements, réseaux, énergie, maintenance et conventions diverses constituent des charges récurrentes souvent sous-estimées. En extérieur, l'usure du matériel est rapide, et l'absence de maintenance rigoureuse peut rendre un système partiellement inexploitable en quelques années.
Enfin, la sécurité du dispositif et sa lisibilité démocratique ne doivent pas être traitées a posteriori. Un système de vidéoprotection doit être conçu comme une infrastructure critique, protégée contre les intrusions numériques et strictement maîtrisée dans ses accès. Parallèlement, assumer une démarche de transparence, notamment par l'information des administrés, contribue à renforcer l'acceptabilité du projet et à prévenir les controverses futures.
Lancer un projet de vidéoprotection n'est donc pas un acte technique, mais une décision de pilotage public. Les choix faits au départ engagent la collectivité bien au-delà du mandat et conditionnent la crédibilité de l'action municipale en matière de sécurité et de gestion du territoire.

6. UN ENVIRONNEMENT DE MENACES ET DE CONTRAINTES PROFONDÉMENT RENOUVELÉ

La vidéoprotection telle qu'elle a été conçue et déployée depuis une vingtaine d'années répondait à un contexte particulier, marqué par des usages majoritairement différés et une logique d'élucidation. Or l'environnement dans lequel les communes exercent aujourd'hui leurs responsabilités a profondément évolué. Les formes de risques, les attentes citoyennes, les contraintes juridiques et la temporalité de l'action publique ne sont plus les mêmes. Continuer à raisonner avec les seuls outils et organisations du passé expose les collectivités à des angles morts croissants.
Pour autant, ce constat ne justifie ni une fuite en avant technologique, ni une remise en cause des équilibres démocratiques posés par le droit. L'enjeu du mandat 2026–2032 est de comprendre ce qui a changé, ce qui relève toujours de la compétence communale, et comment préparer des capacités d'adaptation sans transformer la nature politique des dispositifs existants.

6.1. Évolution des menaces dans l'espace public : événements, foules, nouvelles vulnérabilités

L'espace public est aujourd'hui traversé par des vulnérabilités plus complexes, plus rapides et plus dynamiques qu'auparavant. La multiplication des événements festifs, culturels ou sportifs, l'intensification des flux touristiques, l'évolution des usages quotidiens de la ville et la concentration ponctuelle de foules créent des situations à risque qui ne se réduisent plus à des faits de délinquance classiques. À ces facteurs s'ajoute l'évolution de la menace elle-même, marquée par des modes opératoires simples, mobiles et difficiles à anticiper, comme les attaques au véhicule bélier, l'usage malveillant de drones ou des actions opportunistes de type black bloc dans des espaces ouverts.
Parallèlement, les collectivités sont confrontées à des risques non intentionnels mais tout aussi critiques. Mouvements de foule mal maîtrisés, accidents sur des installations temporaires, dégradations rapides de situations festives, départs de feu, malaises ou chutes dans des espaces très fréquentés, sans oublier l'impact croissant des phénomènes climatiques extrêmes. Dans ces contextes, le facteur temps devient déterminant. La différence entre un incident maîtrisé et une situation de crise tient souvent à la capacité à détecter suffisamment tôt une anomalie et à déclencher une réponse adaptée, dans ce cas, les minutes « peuvent compter triples ».



Ces évolutions s'inscrivent pleinement dans les orientations portées par la Stratégie Nationale de Résilience (SNR) pilotée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN, service du premier ministre). Cette stratégie reconnaît explicitement le rôle des territoires et des collectivités locales dans la capacité globale du pays à anticiper, absorber et surmonter des chocs de nature diverse. Sans transférer aux maires des responsabilités régaliennes, elle leur confère un rôle clé dans la détection précoce, la coordination locale et la continuité des fonctions essentielles à l'échelle communale, dont une résilience forte pour nos concitoyens.
Dans ce cadre, la vidéoprotection classique, historiquement pensée pour l'analyse a posteriori et l'élucidation des faits, montre certaines limites. Elle permet de comprendre ce qui s'est produit, mais pas toujours d'agir à temps face à des situations évolutives ou rapides. Ce constat ne remet pas en cause son utilité, mais met en lumière la nécessité de compléter les dispositifs existants par des organisations et des outils capables de signaler plus tôt des situations anormales, au service de la protection, du secours et de la résilience, sans basculer dans une logique de surveillance généralisée.

6.2. Ce qui relève du maire, ce qui relève de l'État, ce qu'il est dangereux de promettre

Face à ces évolutions, une clarification des responsabilités est indispensable. Le maire conserve des compétences claires en matière de tranquillité publique, de gestion de l'espace communal, de prévention des risques et de protection des personnes et des biens. Il peut agir sur l'organisation locale, les dispositifs de prévention, la coordination des services et l'anticipation de certaines situations dégradées.
En revanche, certaines menaces relèvent clairement de l'État, notamment en matière de renseignement, de lutte antiterroriste ou de maintien de l'ordre à grande échelle. Promettre une capacité communale totale face à des risques qui dépassent ce périmètre est non seulement irréaliste, mais politiquement dangereux. Cela expose les élus à des attentes impossibles à satisfaire et à des critiques sévères en cas d'incident.
La responsabilité politique du maire consiste donc à tenir une ligne claire : agir là où il en a la compétence, coopérer étroitement avec les services de l'État et refuser les promesses excessives. Cette lucidité est une condition essentielle pour bâtir une stratégie crédible et défendable sur la durée d'un mandat.

6.3. Durcissement réglementaire, judiciarisation et responsabilité des décideurs locaux

Parallèlement à l'évolution des menaces, le cadre réglementaire s'est durci. Depuis 2018 et la mise en place du RGPD, les obligations liées à la protection des données, à la transparence, à la traçabilité des décisions et à l'évaluation des dispositifs se sont renforcées. Les élus locaux exercent désormais leurs responsabilités dans un contexte de judiciarisation accrue de l'action publique, où chaque décision peut être contestée, documentée et analysée a posteriori.

Cette évolution impose une rigueur nouvelle dans la conception et l'exploitation des dispositifs de vidéoprotection impliquant désormais le Délégué à la Protection des Données (DPD, ou DPO en anglais). L'improvisation, l'empilement de solutions ou l'absence de documentation ne sont plus soutenables. À l'inverse, un projet bien cadré, juridiquement fondé, gouverné et évalué constitue une protection pour les décideurs eux-mêmes.

Dans ce contexte, ne rien faire peut parfois exposer autant que mal faire. L'absence d'anticipation, de procédures ou de moyens adaptés peut être interprétée comme une carence, notamment lorsqu'un risque était connu ou prévisible. La responsabilité des élus ne se limite plus à l'intention, mais s'apprécie de plus en plus à l'aune de la préparation et de la cohérence des dispositifs mis en place.

6.4. Anticiper sans suréquiper : préparer le terrain des usages futurs sans changer de nature politique



L'enjeu du prochain mandat n'est donc pas d'accumuler des technologies, mais de préparer des capacités. Anticiper ne signifie pas suréquiper, ni céder à des effets de mode. Cela consiste à concevoir des dispositifs évolutifs, proportionnés et compatibles avec les cadres juridiques actuels et à venir.

Préparer le terrain des usages futurs implique d'abord de structurer l'organisation existante : clarifier les chaînes décisionnelles, professionnaliser les opérateurs lorsqu'ils existent, formaliser les procédures et documenter les choix. C'est à cette condition que des outils comme la Remontée Automatique d'Alerte (R2A) pourront, le moment venu, s'intégrer sans rupture politique ou juridique.

Anticiper sans changer de nature politique, c'est aussi poser dès aujourd'hui des lignes rouges claires, en cohérence avec les valeurs démocratiques et le droit européen. Ce n'est pas la technologie qui doit dicter la stratégie, mais la stratégie qui doit encadrer les usages possibles de la technologie. C'est sur cette base que les collectivités peuvent aborder sereinement l'évolution vers des dispositifs plus réactifs, plus ciblés et plus utiles, sans renier les principes posés dans cette première partie de ce livre blanc.



VIDÉOPROTECTION

PARTIE 2 :
DE LA VIDÉOPROTECTION À LA REMONTÉE AUTOMATIQUE D'ALERTE

LECTURE RAPIDE :
COMPRENDRE LES USAGES POSSIBLES, LEURS LIMITES ET LEURS CONDITIONS DE DÉPLOIEMENT

LA DEUXIÈME PARTIE DU LIVRE BLANC A POUR OBJECTIF D'ÉCLAIRER LES ÉLUS SUR LES USAGES CONCRETS DE LA VIDÉOPROTECTION ET DE SES ÉVOLUTIONS POSSIBLES, NOTAMMENT EN MATIÈRE DE REMONTÉE AUTOMATIQUE DE DONNÉES OU D'ALERTES. ELLE NE PROPOSE NI UN CATALOGUE DE SOLUTIONS, NI UNE LISTE DE PROMESSES, MAIS UNE LECTURE STRUCTURÉE DE CE QUI EST TECHNIQUEMENT ENVISAGEABLE, JURIDIQUEMENT DÉFENDABLE ET POLITIQUEMENT PERTINENT SUR UN MANDAT MUNICIPAL.

Le chapitre 7 pose les fondations méthodologiques de cette partie. Il introduit les distinctions essentielles issues des travaux de l'AN2V, en particulier entre remontée automatique de données et remontée automatique d'alerte. Ce chapitre rappelle que ces deux logiques ne répondent ni aux mêmes finalités, ni aux mêmes contraintes juridiques, et qu'elles doivent être clairement différenciées pour éviter les confusions fréquentes entre observation, analyse et intervention. Il constitue une grille de lecture indispensable pour comprendre l'ensemble des cas d'usage présentés ensuite.

Le chapitre 8 constitue le cœur opérationnel de cette partie. Il présente un ensemble de cas d'usage prioritaires pour une commune à l'horizon 2026, couvrant des domaines variés comme la gestion de l'espace public, la sécurité routière, la protection des bâtiments, les atteintes au cadre de vie ou les enjeux environnementaux. Chaque usage est abordé non comme une solution clé en main, mais comme une question à instruire, en tenant compte du contexte local, du zonage des espaces, des objectifs poursuivis et du cadre juridique applicable. Ce chapitre montre que l'image peut être mobilisée au service de politiques publiques très diverses, à condition d'être positionnée de manière proportionnée et gouvernée.

Le chapitre 9 recentre la réflexion sur ce que les collectivités peuvent réellement faire à droit constant dès le début du mandat. Il distingue clairement les usages déjà autorisés, les obligations de conformité à intégrer dès la conception des projets et l'importance de construire une trajectoire opérationnelle plutôt qu'un empilement d'outils. Ce chapitre aide les élus à passer d'une logique d'équipement à une logique de stratégie, adaptée à la taille de la commune, à ses moyens humains et à son niveau de maturité organisationnelle.

Le chapitre 10 ouvre ensuite la perspective du mandat dans la durée. Il présente les évolutions possibles du cadre juridique et réglementaire, notamment au regard de l'IA Act européen, des travaux nationaux en cours et des réflexions sur certains usages spécifiques. L'objectif n'est pas de prédire les futures autorisations, mais d'aider les élus à comprendre ce qui peut évoluer, ce qui doit être préparé dès aujourd'hui et ce qui reste incertain. Ce chapitre invite à une posture de veille active et de prudence stratégique.

Le chapitre 11 aborde les conséquences organisationnelles et humaines de ces évolutions. Il montre que l'introduction de nouveaux usages, en particulier lorsqu'ils reposent sur des alertes ou des analyses automatisées, transforme profondément le rôle des centres de supervision, des opérateurs et des chaînes décisionnelles. Ce chapitre insiste sur l'importance de l'organisation, des compétences et de la conduite du changement, souvent sous-estimées au profit des seules questions technologiques.

Enfin, **le chapitre 12 traite des enjeux d'éthique, de maîtrise des risques et d'acceptabilité** démocratique. Il identifie les risques réels liés aux usages de l'image et de l'automatisation, propose des leviers de prévention et rappelle l'importance de la transparence, de la traçabilité et du dialogue avec les citoyens. Ce chapitre montre que l'acceptabilité ne se décrète pas, mais se construit dans la durée, par une gouvernance claire et un récit public maîtrisé.

DANS SON ENSEMBLE, CETTE DEUXIÈME PARTIE VISE À DONNER AUX ÉLUS UNE VISION RÉALISTE ET STRUCTURÉE DES USAGES ENVISAGEABLES SUR LE MANDAT 2026-2032. ELLE PERMET DE DISTINGUER CE QUI PEUT ÊTRE MIS EN ŒUVRE IMMÉDIATEMENT, CE QUI DOIT ÊTRE PRÉPARÉ AVEC MÉTHODE ET CE QUI RELÈVE ENCORE DE DÉBATS OU D'ÉVOLUTIONS À VENIR. ELLE INVITE À UNE APPROCHE PROGRESSIVE, COHÉRENTE ET ASSUMÉE, LOIN DES EFFETS D'ANNONCE ET DES PROMESSES INTENABLES.

7. DE QUOI PARLE-T-ON VRAIMENT QUAND ON PARLE DE R2A ?

L'entrée dans cette deuxième partie du livre blanc nécessite une clarification préalable. Le terme de Remontée Automatique d'Alerte peut, à première lecture, donner l'impression que l'on se situe exclusivement dans un registre sécuritaire, centré sur la détection d'événements anormaux ou à risque. Cette perception est compréhensible, mais elle ne reflète pas l'ensemble des usages réellement concernés par les dispositifs évoqués dans cette partie.
Les outils abordés ici couvrent en réalité un spectre plus large. Ils permettent à la fois de signaler des situations nécessitant une attention immédiate et de produire aussi, dans la durée, des données utiles à la compréhension et à la gestion du territoire.
Avant d'entrer dans le détail des cas d'usage, il est donc indispensable de poser un cadre sémantique clair, assumé et cohérent avec les enjeux politiques et juridiques du mandat à venir.

7.1. Pourquoi parle-t-on de Remontée Automatique d'Alerte plutôt que «IA» ou «VSA» ?

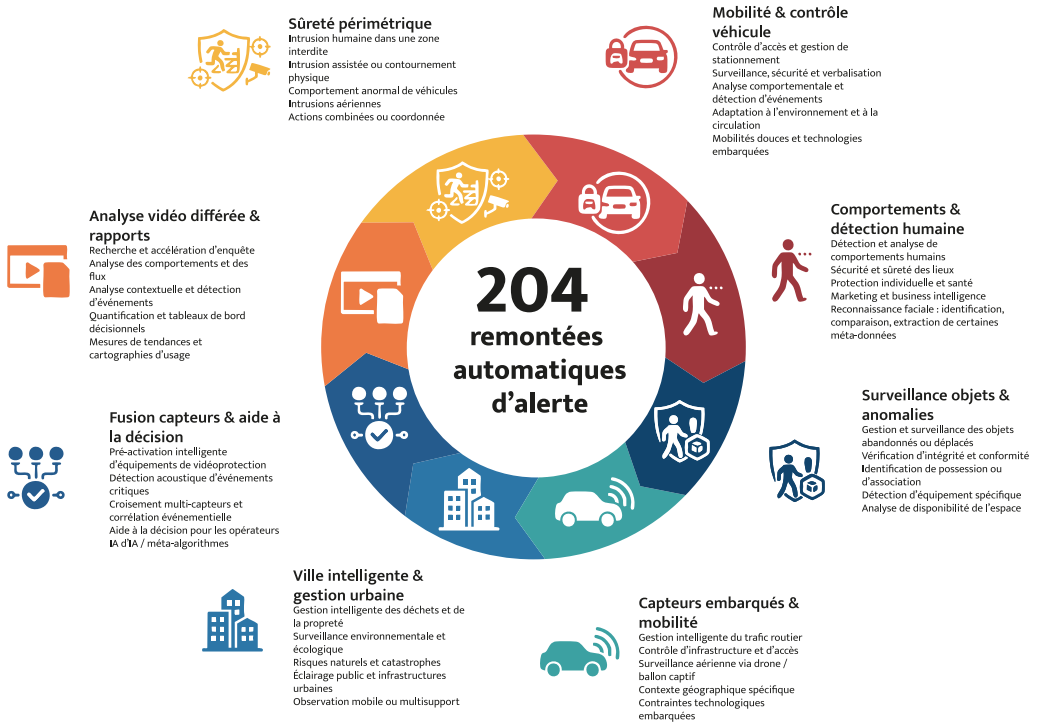
Le choix du terme Remontée Automatique d'Alerte est volontaire. Il permet d'éviter deux écueils majeurs du débat public. Le premier est l'usage générique et anxiogène du terme « intelligence artificielle », devenu un mot-valise qui alimente autant les fantasmes que les peurs. Le second est celui de la « vidéosurveillance algorithmique » ou VSA, expression politisée et volontairement floue, largement utilisée pour entretenir l'idée d'une surveillance généralisée.
Certains acteurs, y compris au sein de l'écosystème AN2V, ont proposé de parler de Remontée Automatique de Données afin d'intégrer explicitement les usages non sécuritaires, comme le comptage de flux piétons ou cyclables, l'analyse de fréquentation d'un espace public, l'observation de l'usage d'un équipement urbain ou le suivi d'indicateurs environnementaux. Cette approche est intellectuellement pertinente, mais elle présente un risque de complexification inutile du discours à destination des élus et du grand public en introduisant in fine deux signifiant plutôt qu'un seul !
Le choix assumé dans ce livre blanc est donc de conserver le terme de R2A, non pas pour réduire ces dispositifs à une logique sécuritaire, mais pour simplifier le débat et neutraliser les amalgames. La R2A désigne ici un principe générique de remontée automatisée d'informations issues de l'analyse d'images, qu'il s'agisse d'alertes sur des situations anormales ou de données agrégées utiles à la gestion du territoire. Ce choix permet de sortir du champ lexical de la VSA et de l'IA fantasmée, tout en conservant une lecture opérationnelle et juridiquement maîtrisée.

7.2. Le principe fondamental : détecter des situations, pas des identités

Le principe fondamental reste inchangé et constitue une ligne rouge absolue. Les dispositifs regroupés sous le terme de R2A visent à analyser des situations observables dans l'espace public, non à identifier des individus. Qu'il s'agisse de déclencher une alerte ou de produire des données statistiques, l'objet de l'analyse est toujours un événement, un usage ou une dynamique, jamais une identité, ou autrement dit juridiquement, une donnée biométrique.
Dans le registre de l'alerte, il peut s'agir de signaler une chute d'une personne ou d'une lourde branche d'arbre, un attroupement inhabituel, un véhicule en situation dangereuse ou à contresens, un départ de feu ou une montée anormale des eaux. Dans le registre de la donnée, il peut s'agir de compter des piétons dans une rue commerçante, d'évaluer l'usage d'une piste cyclable, de mesurer la fréquentation d'une place lors d'un événement ou d'observer l'utilisation d'un équipement de tri sélectif. Dans les deux cas, aucune reconnaissance individuelle n'est recherchée, ni nécessaire et en tout état de cause, il s'agit toujours d'alerter un opérateur de vidéoprotection qui prend la décision de la suite à donner.
Cette approche permet de privilégier des usages simples, utiles et immédiatement exploitables, selon une logique pragmatique dite 80/20, loi de Pareto. L'objectif n'est pas d'exploiter toutes les capacités théoriques des technologies disponibles, mais de produire rapidement de la valeur pour les collectivités, qu'il s'agisse de protection, de secours, de gestion urbaine ou de pilotage des politiques publiques.

7.3. Différence entre vidéosurveillance, vidéoprotection et R2A

La Remontée Automatique d'Alerte, au sens large retenu dans ce document, ne se substitue ni à la vidéoprotection ni aux dispositifs existants, c'est un complément : Elle s'y superpose comme une couche fonctionnelle supplémentaire. La vidéoprotection reste le cadre juridique de captation et d'exploitation des images sur la voie publique ou dans les espaces ouverts au public, avec ses finalités, ses autorisations et ses contraintes propres.
La R2A intervient en complément de l'exploitation humaine des images. Elle peut signaler automatiquement une situation nécessitant une attention particulière ou produire des données agrégées issues de l'observation continue d'un espace. Dans les deux cas, elle ne modifie ni la nature des images captées, ni les règles de conservation (30 jours), ni les droits d'accès. Elle agit comme un outil d'aide à l'attention pour l'opérateur du CSU, CSUi ou CSD et à l'analyse, là où un traitement purement humain serait matériellement impossible donc inefficace.
Il est donc essentiel de comprendre que la R2A n'est pas un dispositif autonome. Sans organisation humaine, sans gouvernance claire et sans finalités explicitement définies, elle n'a aucun sens opérationnel ni politique.



7.4. Ce que la R2A ne fait pas et ne fera pas dans le cadre juridique européen et national

Enfin, il est indispensable de rappeler ce que la R2A, telle qu'entendue dans ce livre blanc, ne fait pas et ne fera pas. Le cadre juridique européen et national fixe des limites claires, qui excluent toute dérive vers une surveillance de masse ou une identification automatisée des personnes.
Le règlement européen sur l'intelligence artificielle (IA Act) interdit notamment la reconnaissance faciale en temps réel à des fins d'identification généralisée dans l'espace public. Les dispositifs de suivi permanent des individus, de constitution de bases biométriques ou de surveillance indifférenciée sont proscrits. Ces interdictions sont explicites, elles ont déjà été votées, et ne laissent pas place à

des interprétations extensives ou évolutions envisageables.
La R2A ne permet donc ni d'identifier des personnes, ni de les suivre, ni de croiser des données individuelles. Elle ne décide pas, ne sanctionne pas et ne se substitue pas aux autorités compétentes. Qu'elle produise une alerte ou une donnée statistique, elle reste un outil d'aide, encadré, traçable et gouverné.
Clarifier ces limites dès le début de cette Partie 2 est essentiel. Cela permet de recentrer le débat sur les usages réellement envisageables, utiles et acceptables pour les collectivités, et de sortir durablement des peurs entretenues par la confusion volontaire entre technologie, surveillance et décision politique.

7.5. Synthèse des usages envisageables issus des travaux de l'AN2V

Les travaux menés au sein du groupe de travail de l'AN2V consacré aux usages de l'intelligence artificielle, devenu groupe de travail « R2A » depuis décembre, ont permis d'identifier et de structurer un ensemble représentatif de cas d'usage à considérer. Cette synthèse propose une lecture consolidée des principaux scénarios analysés, en tenant compte à la fois des réalités opérationnelles des territoires et des cadres juridiques et institutionnels en vigueur.

8. DIX À QUINZE CAS D'USAGE PRIORITAIRES POUR UNE COMMUNE EN 2026

Les cas d'usage présentés dans ce chapitre répondent à une attente potentiellement forte des élus locaux : comprendre ce qui est techniquement envisageable, politiquement pertinent et juridiquement défendable à l'horizon du mandat 2026–2032. Ils doivent être lus avec une grille de lecture claire, issue des travaux menés au sein de l'AN2V, et qui seront expliqués à nouveau dans le cadre des universités « 1 jour pour 5 ans » à Chartres le 23 juin 2026. L'approche dite « 1J5A » signifie qu'en une seule journée, organisée à Chartres dans le cadre des universités de l'AN2V, il sera possible de parcourir et de mettre en perspective cinq années de projets potentiels, correspondant à la durée d'un mandat municipal.
Trois distinctions sont essentielles :

- La première concerne la nature de la remontée.
  - R2A : Une remontée automatique d'alerte s'inscrit dans une logique de sécurité et vise à signaler une situation anormale ou atypique nécessitant une attention immédiate.
  - R2D : Une remontée automatique de données, à l'inverse, produit des informations statistiques ou agrégées, sans déclenchement d'alerte ni qualification d'anomalie.

  Ces deux logiques ne relèvent ni des mêmes usages, ni des mêmes contraintes juridiques.
- La deuxième distinction concerne les espaces juridiques. Les usages n'ont pas le même statut selon qu'ils s'exercent en **espace public** (zone bleue), en **espace privé ouvert au public** comme un ERP (zone orange), ou en **espace privé strict** (zone verte). C'est souvent moins la technologie que l'espace concerné qui détermine la faisabilité juridique.



- Enfin, il convient de rappeler qu'à la date de rédaction de ce livre blanc, les usages reposant sur une logique de remontée automatique d'alerte en espace public ne disposent pas encore d'un cadre juridique stabilisé en droit commun. Ces usages ne sont pas, à ce stade, rattachés aux finalités du Code de la sécurité intérieure permettant au préfet d'autoriser le déploiement d'un dispositif sur la voie publique. À l'inverse, les usages fondés sur la remontée de données simples, strictement statistiques et sans déclenchement d'alerte, s'inscrivent dans une logique différente. Ils peuvent être envisagés dès lors qu'ils font l'objet d'une analyse d'impact rigoureuse et d'une validation explicite par le Délégué à la Protection des Données de la collectivité.

8.1. Comptage et statistiques

Le comptage et la production de statistiques constituent souvent le premier usage envisagé par les communes, car ils répondent à un besoin simple : connaitre son territoire et objectiver des choix publics : Compter les piétons dans une rue commerçante, les vélos sur une piste cyclable ou les véhicules sur un axe structurant permet d'évaluer une politique de mobilité, d'urbanisme (rédaction d'un Plan de Mobilité – PDM) ou de revitalisation sans entrer dans une logique sécuritaire.
Ces usages relèvent clairement d'une logique de remontée de données. En espace public et en espace privé ouvert au public, ils peuvent être envisagés à condition de rester strictement statistiques, agrégés dans le temps et dépourvus de toute qualification d'anomalie ou d'événement, et encore moins de données personnelles à caractère biométrique. En espace privé strict, ils relèvent pleinement de la gestion interne du site. À l'inverse, toute tentative de transformer ces données en alertes automatiques bascule dans une logique différente, qui ne dispose pas encore d'un cadre juridique stabilisé.

8.2. Gestion et optimisation des territoires «connectés et durables» et des espaces publics

De nombreuses collectivités cherchent aujourd'hui à mieux comprendre l'usage réel de l'espace public afin d'objectiver leurs décisions et d'optimiser leur action. La vidéoprotection, lorsqu'elle est utilisée dans une logique de remontée de données et non d'alerte, peut devenir un véritable outil d'aide à la décision publique. Il peut s'agir de mesurer des congestions récurrentes, d'analyser l'occupation d'une place, d'évaluer l'impact d'un nouvel aménagement, d'ajuster une signalisation ou d'objectiver des choix en matière de stationnement et de mobilités.
Sur **l'espace public**, en **zone bleue**, ces usages doivent rester strictement descriptifs et non événementiels. La caméra agit alors comme un observatoire du territoire, produisant des indicateurs globaux de fonctionnement utiles à la planification, à l'évaluation des politiques publiques et à l'adaptation des aménagements urbains. Dans cette logique, certaines collectivités explorent également des usages liés à l'observation de phénomènes environnementaux ou naturels, dès lors qu'ils restent agrégés, non intrusifs et juridiquement sécurisés.
Dans les **espaces privés ouverts au public**, en **zone orange**, comme les bâtiments communaux, bibliothèques, piscines ou annexes de mairie, les marges de manœuvre sont plus larges. Les caméras peuvent y être mobilisées comme capteurs de données permettant une gestion fine des affluences et une optimisation du fonctionnement des équipements. L'ajustement de l'éclairage, du chauffage ou de la ventilation en fonction de l'occupation réelle contribue à la fois à la maîtrise des coûts, à la performance énergétique et à une gestion plus responsable du patrimoine public, sans basculer dans une logique sécuritaire excessive.
Enfin, dans les **espaces privés stricts**, en **zone verte**, ces dispositifs relèvent pleinement d'une logique d'optimisation interne. Ils peuvent soutenir le pilotage énergétique des bâtiments, faciliter une maintenance plus préventive des installations techniques ou améliorer l'organisation des flux et des usages internes. Dans ce périmètre maîtrisé, le recours à des alertes automatiques ciblées de type R2A, par exemple en cas d'intrusion ou d'anomalie technique, peut être envisagé dans un cadre juridique et organisationnel clairement défini et validé par le DPD.
Ces usages, centrés sur la gestion, la performance et la durabilité, illustrent que la vidéo n'est pas uniquement un outil de sécurité. Lorsqu'elle est correctement positionnée, gouvernée et expliquée, elle devient un levier discret mais structurant de pilotage des politiques territoriales, au service de décisions plus rationnelles et plus efficaces.

8.3. Détection de chutes, malaises, noyades et personnes au sol

La détection automatique d'une chute, d'un malaise ou d'une noyade correspond typiquement à une remontée automatique d'alerte, orientée vers la sécurité et le secours. Elle vise à signaler une situation critique nécessitant une réaction rapide.
En espace public, ce type d'usage ne dispose pas encore d'un cadre juridique stabilisé en droit commun, l'AN2V consacre une grande énergie pour que cette anomalie du droit juridique cesse, dès le mandat 2026-2032. En espace privé ouvert au public, comme une piscine municipale ou un équipement sportif, la question peut se poser différemment, sous des conditions strictes et une gouvernance claire (mise sous alarme la nuit par exemple). En espace privé strict, elle relève da-

vantage de la sûreté et de la responsabilité de l'exploitant. Ce que les communes peuvent d'ores et déjà renforcer, en revanche, ce sont les organisations humaines, les procédures d'intervention et la supervision, en utilisant l'image comme support d'aide à la décision sans automatisation de l'alerte (lever de doute).

8.4. Départs de feu, fumées anormales et risques dans les équipements

La détection d'un départ de feu ou d'une fumée anormale est souvent perçue comme un usage consensuel, car elle cible un phénomène physique et non un comportement humain. Lorsqu'elle repose sur une logique d'alerte automatique, elle relève néanmoins d'une remontée d'alerte de sécurité ! Et souvenez-vous, cette R2A était clairement stipulée dans l'expérimentation des JOP2024 comme étant un des huit usages à expérimenter ce qui prouve le besoin de poursuivre les efforts juridiques et de modification du CSI !

En revanche, lorsque le projet est explicitement porté par la Direction générale de la sécurité civile et de la gestion des crises (DGSCGC), et que les caméras sont utilisées exclusivement à des fins de détection pour la prévention et la détection des feux de forêt, dans des dispositifs dédiés intégrant des caméras qui pivotent doucement sur leur axe à 360 degrés, avec également des capteurs thermiques, cet usage s'inscrit clairement dans un cadre autorisé.

8.5. Mouvements de foule, attroupements dangereux, évènements festifs

La détection automatique d'un attroupement ou d'un mouvement de foule vise à anticiper des situations de tension ou de danger lors d'événements festifs ou de forte affluence. Elle relève clairement d'une logique de remontée d'alerte orientée sécurité, donc de R2A.

En espace public, ce type d'usage ne peut pas être présenté comme déployable en droit commun à ce jour. Ce qui relève pleinement de la responsabilité communale, en revanche, c'est la préparation des événements, la supervision humaine, la mutualisation des centres de supervision, la coordination avec les services de l'État et l'usage des images comme outil d'appui à la décision, sans automatisation de l'alerte mais avec des opérateurs devant les écrans !

8.6. Sécurité routière : contresens, stationnement dangereux, voies douces

La sécurité routière repose sur la capacité des collectivités à identifier et à prévenir les situations à risque avant qu'elles ne se traduisent par des accidents. L'évolution des usages de l'espace public et la cohabitation de modes de déplacement hétérogènes font apparaître des configurations sensibles, notamment les circulations à contresens, le stationnement dangereux et l'occupation inappropriée des voies dédiées aux mobilités douces.

Les circulations à contresens se manifestent le plus souvent dans des contextes urbains complexes, rues à sens unique, zones de travaux, accès à des équipements ou carrefours contraints, où la signalisation et l'aménagement montrent leurs limites. Leur dangerosité tient à leur caractère imprévisible et au potentiel de gravité des accidents qu'elles peuvent provoquer. De manière comparable, le stationnement dangereux perturbe les trajectoires, réduit la visibilité et expose directement les usagers les plus vulnérables. Ces situations traduisent rarement des comportements isolés ; elles révèlent plus souvent une inadéquation entre l'organisation de la voirie et les usages réels.

Les voies dédiées aux mobilités douces s'inscrivent dans cette même dynamique. Conçues pour protéger des usagers particulièrement exposés, elles ne remplissent leur fonction que si leur vocation est clairement lisible et respectée. Leur occupation ponctuelle ou répétée par des véhicules motorisés fragilise la sécurité des déplacements et génère des situations de conflit.

Dans ce contexte, l'usage de l'image peut constituer un outil d'appui à la compréhension des situations à risque, à condition d'être clairement positionné et juridiquement encadré. La distinction entre R2D, à visée descriptive et préventive, et R2A plus contraignante et juridiquement limitée en espace public, demeure centrale. Utilisée de manière proportionnée, l'image peut contribuer à objectiver les situations et à éclairer l'action publique, sans se substituer aux autres leviers de la sécurité routière ni remettre en cause les libertés publiques.

8.7. Risques naturels et technologiques : inondations, crues, submersions, incendies

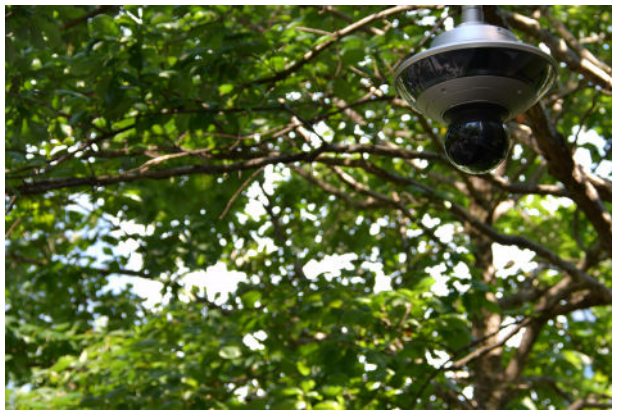
Les risques naturels et technologiques constituent désormais un axe central de l'action publique locale. Les étés récents, et en particulier l'été 2025, ont été marqués par une intensification des phénomènes extrêmes, avec des incendies atteignant des zones périurbaines et parfois urbaines. Plus de 36 000 hectares ont ainsi été détruits en France depuis le début de l'année 2025, selon le système européen d'information sur les feux de forêt. À ces incendies s'ajoutent des épisodes de crues soudaines, d'inondations, de submersions marines, de tempêtes ou de vagues de chaleur, dont la fréquence et l'intensité s'inscrivent durablement dans le contexte du changement climatique.

Ces évolutions ne relèvent plus de l'exception. Elles s'inscrivent pleinement dans la Stratégie nationale de résilience (SNR) portée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), qui fixe un cadre clair : la capacité du pays à faire face au mieux aux crises repose en grande partie sur la préparation, l'anticipation et la coordination à l'échelle territoriale. Dans cette stratégie, les collectivités locales, et en particulier les communes, ne sont pas de simples relais, mais des acteurs à part entière de la résilience, en charge de la continuité des fonctions essentielles et de la protection des populations.

Dans ce cadre, l'usage de l'image peut contribuer à renforcer la capacité d'anticipation et de gestion des risques, à condition d'être correctement positionné. L'observation continue de cours d'eau, de zones littorales, de points bas, de massifs forestiers ou d'infrastructures exposées relève d'une logique de remontée de données (R2D). Elle permet de documenter l'évolution de phénomènes, d'objectiver des seuils de vigilance et d'alimenter les plans communaux de sauvegarde et les dispositifs de prévention. En espace public, cette approche reste envisageable dès lors qu'elle demeure descriptive, sans déclenchement automatique d'alerte, et qu'elle s'inscrit dans une gouvernance claire et proportionnée.

La détection automatique d'un départ de feu, d'une montée rapide des eaux ou du franchissement d'un seuil critique correspond en revanche à une logique de remontée automatique d'alerte, orientée sécurité et gestion de crise. En espace public, ce type d'usage ne dispose pas encore d'un cadre juridique stabilisé lorsqu'il est porté à l'initiative d'une commune sur les caméras de vidéoprotection soumises à une autorisation préfectorale. Il doit donc être abordé comme une perspective d'évolution ou un champ d'expérimentation, et non comme une capacité immédiatement déployable dans le cadre d'un programme municipal, ou avec une extrême prudence, à voir avec la Commission Départementale de Vidéoprotection (CDV), le référent sûreté GN ou PN de votre commune, le Préfet du Département...

Il existe toutefois des configurations spécifiques dans lesquelles ces dispositifs s'inscrivent dans un cadre autorisé. Lorsque les projets sont explicitement portés par l'État, notamment par la Direction générale de la sécurité civile et de la gestion des crises, et qu'ils sont dédiés à des missions ciblées comme la détection des feux de forêt, avec des équipements spécialisés tels que des caméras à 360 degrés ou des capteurs thermiques, l'usage de la détection automatisée s'inscrit dans un cadre distinct. Dans ces situations, les communes peuvent être partenaires, contributrices ou bénéficiaires des dispositifs, sans en assumer seules la responsabilité juridique.



Enfin, l'image joue un rôle essentiel dans la gestion de crise indépendamment de toute automatisation de l'alerte. La supervision humaine, la coordination des services municipaux, le suivi des moyens engagés et la mise en cohérence des informations issues de différents capteurs participent à une logique d'hypervision territoriale, pleinement cohérente avec les objectifs de la Stratégie nationale de résilience. Ces usages, centrés sur l'aide à la décision et la coordination, relèvent

aujourd'hui pleinement des responsabilités communales, à condition d'être intégrés dans une organisation de crise structurée, documentée et partagée avec les acteurs de l'État.
Il convient toutefois de ne pas surévaluer le rôle des dispositifs technologiques dans des scénarios de crise de grande ampleur. L'expérience des événements récents montre que, lors de situations extrêmes, les premières vulnérabilités concernent souvent les infrastructures essentielles, au premier rang desquelles l'alimentation énergétique. Coupures électriques, instabilité des réseaux moyenne et haute tension, défaillances des télécommunications ou saturation des réseaux mobiles conduisent fréquemment à une perte rapide de fonctionnement des systèmes numériques, parfois en quelques dizaines de minutes ou quelques heures. La Stratégie nationale de résilience rappelle régulièrement que la continuité de l'énergie, qu'il s'agisse du réseau basse, moyenne ou haute tension, constitue un prérequis absolu à toute ambition technologique. Sans sécurisation des sources d'alimentation, des redondances et des plans de continuité, les dispositifs les plus avancés deviennent inopérants au moment même où ils seraient le plus utiles.

8.8. Dépôts sauvages et atteintes à l'environnement

Les dépôts sauvages constituent une problématique croissante pour les collectivités, tant par leurs impacts sur le cadre de vie que par les coûts qu'ils génèrent en matière de nettoyage, de maintenance et de suivi administratif. Au-delà de la nuisance visuelle et du sentiment d'abandon qu'ils provoquent, certains dépôts présentent des risques environnementaux et sanitaires significatifs, notamment lorsqu'ils contiennent des déchets dangereux ou polluants, comme des matériaux amiantés ou des substances toxiques, susceptibles d'affecter durablement les sols, l'eau ou la biodiversité.
Ces enjeux expliquent l'attention croissante portée à ce sujet par les services de l'État, en particulier ceux rattachés au ministère en charge de la transition écologique. Les dépôts sauvages ne relèvent plus uniquement de la propreté urbaine ou de l'incivilité, mais s'inscrivent désormais dans une logique de protection de l'environnement et de gestion des risques. Dans ce contexte, les stratégies classiques, fondées sur la dissuasion ponctuelle ou la verbalisation a posteriori, montrent rapidement leurs limites, notamment face à la difficulté d'identification des auteurs et à la récurrence des phénomènes.
L'usage de l'image peut, dans ce cadre, constituer un outil d'appui, à condition d'être strictement ciblé, proportionné et juridiquement encadré. Il ne s'agit pas de surveiller en continu l'espace public, mais d'objectiver des situations récurrentes sur des zones identifiées, afin d'améliorer la réactivité des services, de prioriser les interventions et, lorsque le cadre le permet, d'appuyer les procédures prévues par la loi. Ces dispositifs relèvent prioritairement de logiques de remontée de données, et non d'alerte généralisée.
Pour les élus, l'enjeu est également prospectif. Les atteintes environnementales liées aux dépôts sauvages font l'objet de réflexions et d'évolutions réglementaires en cours, susceptibles d'impacter à terme les conditions d'usage de dispositifs de détection ou de signalement automatisés. Il est donc essentiel de suivre de près les évolutions juridiques, notamment celles relatives aux dispositifs de R2A, afin d'anticiper les cadres futurs sans s'exposer à des usages prématurés ou fragiles juridiquement.
Ainsi positionnée, la lutte contre les dépôts sauvages s'inscrit dans une politique publique globale de protection de l'environnement et du cadre de vie. L'image, utilisée comme outil d'appui et d'objectivation, peut renforcer l'efficacité de l'action municipale, sans basculer dans une logique de surveillance généralisée ni remettre en cause les principes fondamentaux de respect des libertés publiques.

8.9. Protection des bâtiments publics sensibles et des abords

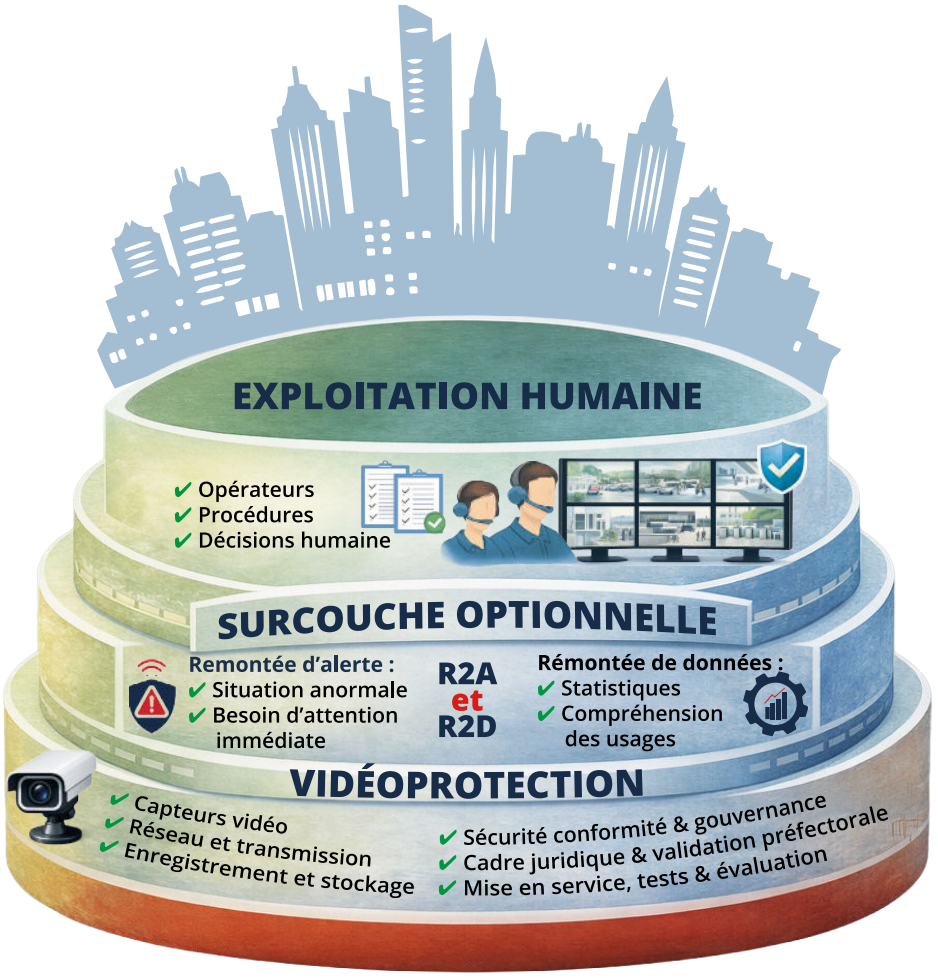
La protection des bâtiments publics illustre particulièrement bien l'importance de la distinction des espaces juridiques. Selon que l'on se situe en espace public, en espace privé ouvert au public ou en espace privé strict, les usages et les marges de manœuvre de la collectivité ne sont pas les mêmes. C'est souvent moins la technologie mobilisée que la nature de l'espace concerné qui détermine la faisabilité juridique des dispositifs envisagés, et c'est précisément l'une des spécificités d'un bâtiment public que de concentrer, sur un même site, ces trois zones distinctes.
En pratique, l'espace public correspond à la zone dite « bleue », qui inclut les rues, les places et aussi les abords immédiats du bâtiments, son parking etc. À ce titre, l'autorisation préfectorale porte classiquement sur la visualisation et l'enregistrement des images, dans les conditions prévues par le Code de la sécurité intérieure, notamment en matière de durée de conservation (maxi 30 jours).
Les espaces privés ouverts au public, comme les halls ou les salles accessibles d'une mairie, d'une école ou d'un équipement municipal, relèvent de la zone « orange » et appellent un encadrement renforcé, notamment en matière d'information du public et de proportionnalité des usages (Cf. les fiches CNIL pour les implantation dans une école par exemple).
Les espaces privés stricts, enfin, tels que les zones techniques, les réserves ou les locaux à accès restreint, constituent la zone « verte », dans laquelle la collectivité dispose d'une marge de manœuvre plus large pour des usages de sécurité et de gestion, sous le contrôle du responsable de traitement et du Délégué à la Protection des Données, qui doivent éventuellement être « bousculés » afin de sortir de la zone où ne placer aucun dispositif, ni de R2A, est la solution la plus simple et la plus sûre !
Concernant les abords immédiats des bâtiments publics, il s'agit d'une bande de quelques mètres autour du bâtiment à protéger, intégrée à l'espace public mais directement liée à la protection du site. Dans le cadre d'une autorisation préfectorale, ces abords peuvent être inclus pour une simple visualisation et un enregistrement des images dans les limites réglementaires. Tant que les usages se limitent à des mesures statistiques ou à une observation descriptive relevant d'une logique de remontée de données, ils ne soulèvent pas de difficulté particulière. En revanche, le passage à une logique de remontée automatique d'alerte sur ces abords, qu'il s'agisse de détecter un comportement suspect ou un départ de feu, demeure, à ce stade, contraint par le cadre juridique en vigueur et ne peut pas être généralisé.

9. CE QUE LES COLLECTIVITÉS PEUVENT FAIRE À DROIT CONSTANT DÈS LE DÉBUT DU MANDAT

À l'issue des chapitres précédents, une confusion doit être levée. Le fait que certains usages de remontée automatique d'alerte ne disposent pas encore d'un cadre juridique stabilisé en espace public ne signifie pas que les collectivités doivent rester immobiles en début de mandat. À droit constant, de nombreuses actions peuvent être engagées immédiatement, à condition de respecter les périmètres juridiques, de clarifier les objectifs, de structurer l'organisation et de prendre en compte qu'à tout moment sur le mandat, le champs des possibles va s'ouvrir.
Ce chapitre vise donc à identifier ce qui peut être fait sans attendre une évolution du cadre législatif, en distinguant clairement les usages autorisés, les obligations associées et les trajectoires réalistes selon la taille des communes.

9.1. Ce que les collectivités peuvent faire à droit constant dès le début du mandat

À droit constant, les collectivités peuvent s'appuyer sur trois leviers principaux.
Le premier concerne les usages de vidéoprotection classique et les exploitations humaines des images en temps réel et/ou en temps différé (relecture), dans le strict respect du Code de la sécurité intérieure. Observation, visualisation, enregistrement, relecture a posteriori et exploitation à des fins d'élucidation ou d'aide à la décision restent pleinement autorisés lorsqu'ils sont proportionnés, justifiés et encadrés.
Le deuxième levier concerne les usages de remontée de données strictement statistiques, sans déclenchement d'alerte ni qualification d'anomalie. Comptages, analyses de flux, mesures d'usage de l'espace public ou d'équipements peuvent être envisagés dès lors qu'ils sont conçus de manière non intrusive, agrégée et validée par le Délégué à la Protection des Données.
Enfin, les espaces privés stricts et les sites maîtrisés constituent un champ d'action plus large pour les collectivités, notamment pour des usages de sécurité interne ou de gestion, sous réserve d'une gouvernance claire et d'un respect rigoureux du cadre RGPD.



LA R2A DÉTECTE DES SITUATIONS, JAMAIS DES IDENTITÉS

9.2. Les obligations de conformité à intégrer dès la conception

Toute démarche engagée dès le début du mandat doit intégrer les exigences de conformité, non comme une contrainte a posteriori, mais comme un élément structurant du projet. L'analyse d'impact relative à la protection des données (AIPD) constitue un outil central. Elle permet de qualifier les finalités, d'identifier les risques, de documenter les choix et la circulation de la donnée, de sécuriser juridiquement les décideurs.

Au-delà de l'AIPD, les collectivités doivent être attentives aux durées de conservation des images et des données, des métadonnées (données détectées dans les images), aux modalités d'information du public, au droit d'accès à l'image par le citoyen et à la documentation des décisions. Ces éléments sont souvent perçus comme techniques, mais ils conditionnent la robustesse juridique et politique des dispositifs sur la durée du mandat.

9.3. Construire une trajectoire opérationnelle plutôt qu'un empilement d'outils

À droit constant, la question n'est donc pas de savoir quelle technologie acheter, mais quelle trajectoire construire et de phaser les déploiements au travers d'un schéma directeur. Cette trajectoire dépend étroitement de la taille de la commune, de ses moyens humains, de son exposition aux risques et de son niveau de maturité organisationnelle.

Plutôt que de viser d'emblée des dispositifs complexes, les collectivités ont intérêt à renforcer progressivement leur organisation, leur gouvernance et leur capacité à exploiter utilement les images et les données existantes. C'est cette préparation qui permettra, le moment venu, d'intégrer de nouveaux usages sans rupture juridique ou politique.

9.4. Exemples de trajectoires opérationnelles dès 2026-2027 selon la taille de la commune

9.4.1. Communes de moins de 2 000 habitants

Pour les petites communes, l'enjeu principal n'est pas technologique mais avant tout organisationnel. À droit constant, la priorité consiste à sécuriser quelques sites sensibles, à s'appuyer sur une vidéoprotection simple et proportionnée, éventuellement mutualisée à l'échelle intercommunale ou à défaut pensée comme telle, et à structurer une relation claire et régulière avec les services de l'État, notamment au travers du référent sûreté de la police nationale ou de la gendarmerie nationale.

Dans ce contexte, le recours à des caméras dites « nomades » peut constituer une réponse adaptée. Leur capacité à être déplacées régulièrement, par exemple d'une semaine à l'autre, en fonction d'un événement, d'une fête locale ou d'une problématique ponctuelle, permet de couvrir différents secteurs du territoire sans multiplier les équipements fixes et les liens réseau à créer. Cette souplesse d'usage renforce l'efficacité du dispositif, tant en matière de prévention que d'élucidation, en introduisant un effet de variabilité qui limite les comportements d'adaptation.

Les usages pertinents portent prioritairement sur l'élucidation des faits, la prévention situationnelle et la remontée de données simples, permettant d'objectiver des problématiques locales récurrentes. À ce stade, toute promesse de remontée automatique d'alerte en temps réel serait à la fois irréaliste sur le plan opérationnel et fragile sur le plan juridique. Dans une organisation strictement communale, la logique de R2A demeure donc largement hors sujet en début de mandat.

9.4.2. Communes autour de 5 000 à 10 000 habitants

Pour les communes d'environ 5 000 habitants ou plus, la logique reste proche de celle des plus petites collectivités, mais avec une capacité accrue à structurer l'organisation et à professionnaliser l'exploitation des dispositifs. L'enjeu n'est toujours pas de multiplier les technologies, mais de consolider un fonctionnement plus régulier, plus lisible et plus efficace dans le temps.

À ce stade, la commune peut envisager la mise en place d'un véritable point central de visualisation, même de taille modeste, s'apparentant à un premier niveau de centre de supervision urbain (CSU). Il ne s'agit pas nécessairement d'un fonctionnement en continu, mais d'une organisation permettant de mobiliser un ou plusieurs opérateurs dédiés sur des plages horaires définies chaque semaine, à la fois pour la prévention, la scrutation ciblée et la relecture des images. Cette capacité humaine constitue un saut qualitatif important par rapport à une exploitation ponctuelle ou exclusivement a posteriori du chapitre précédent.

Cette montée en charge permet également d'introduire une analyse plus structurée des données issues du dispositif, dans une logique de remontée de données simples (R2D). L'observation des flux, la compréhension des usages de l'espace public ou l'objectivation de phénomènes récurrents deviennent alors exploitables dans le temps, sans basculer dans une logique d'alerte automatique. Le dispositif commence ainsi à produire de la valeur au-delà de la seule élucidation, tout en restant pleinement compatible avec le cadre juridique existant.

Enfin, les communes de cette taille sont en mesure de se projeter dans une logique de mutualisation plus aboutie. Elles peuvent soit porter un centre de supervision intercommunal (CSUi) à l'échelle du bloc communal, soit s'inscrire comme partenaire ou client d'un dispositif existant dans une commune voisine plus importante. Cette approche permet d'anticiper une montée en puissance future, tant organisationnelle que fonctionnelle, et de préparer l'intégration progressive de nouveaux usages lorsque le cadre juridique le permettra, à l'image de ce qui est en cours de discussion en R2A comme la Lecture Automatique de Plaques d'Immatriculation (LAPI).

9.4.3. Communes de plus de 20 000 habitants

À partir de ce seuil, la commune entre pleinement dans une logique de continuum de sécurité, telle qu'introduite par la loi de « sécurité globale préservant les libertés » de 2021. Ce concept repose sur une idée simple mais structurante : la sécurité du territoire ne relève plus d'acteurs isolés, mais d'une chaîne continue associant l'État, les collectivités, les polices municipales, les services de secours et, le cas échéant, les dispositifs de mutualisation intercommunale.

Pour une commune de plus de 20 000 habitants, cette logique se traduit par une responsabilité accrue dans l'organisation quotidienne de la sécurité, de la tranquillité publique et de la résilience du territoire. La question n'est plus de savoir s'il faut structurer un dispositif, mais de le faire de manière permanente, lisible et robuste, capable de fonctionner de jour comme de nuit, en situation courante comme lors d'événements festifs, de crises climatiques ou d'incidents majeurs.

Dans ce contexte, la mise en place d'un centre de supervision urbain pleinement opérationnel constitue un socle indispensable, idéalement en h24 et 365j/an. Ce CSU doit s'inscrire clairement dans le continuum de sécurité, en articulation avec les forces de sécurité intérieure et les services de secours. Il repose sur des personnels formés, salariés et identifiés, capables d'assurer la visualisation en temps réel, la relecture rapide des images, la transmission d'informations qualifiées et la coordination opérationnelle. La valeur du dispositif ne tient pas à la technologie, mais à la capacité humaine à interpréter, décider et agir dans un cadre partagé.

Cette structuration permet également d'installer une stratégie cohérente de remontée de données simples à l'échelle de la commune. L'analyse des flux, des usages de l'espace public, des périodes de tension ou des phénomènes récurrents peut alimenter le pilotage global du territoire, en lien avec les politiques de mobilité, de prévention et de gestion des risques. Ces usages s'inscrivent pleinement dans le cadre juridique existant, dès lors qu'ils sont proportionnés, documentés et validés par le Délégué à la Protection des Données.

Les communes de cette taille ont par ailleurs vocation à jouer un rôle structurant au sein du bloc communal. Dans une logique de continuum de sécurité, elles peuvent se positionner comme porteuses d'un centre de supervision intercommunal, en mettant leurs capacités opérationnelles au service des communes voisines de 2 000 ou 5 000 habitants des deux chapitres précédents ! Cette mutualisation permet d'assurer une continuité de service et une capacité de réaction que les petites communes ne peuvent atteindre seules, tout en renforçant la cohérence territoriale.

Enfin, une commune de plus de 20 000 habitants doit se préparer, sans les déployer prématurément, aux évolutions futures des usages de remontée automatique d'alerte lorsque le cadre juridique le permettra. Cette préparation relève pleinement du continuum de sécurité : elle passe par la structuration des procédures, la formation des opérateurs, la clarification des chaînes décisionnelles et l'articulation avec l'État. À l'image de la montée en puissance progressive de dispositifs comme le LAPI, l'enjeu n'est pas d'annoncer des capacités hors cadre, mais d'être prêt, le moment venu, sans doute dès ce mandat, à les intégrer de manière responsable, proportionnée et respectueuse des règles juridiques.

9.4.4. Communes de plus de 100 000 habitants

Pour les communes de plus de 100 000 habitants, généralement situées en zone police nationale, la logique change encore d'échelle. À ce niveau, le fonctionnement en continu du dispositif de supervision n'est plus une option mais une nécessité. Le centre de supervision urbain doit être conçu pour fonctionner 24 heures sur 24, 365 jours par an, en capacité d'absorber aussi bien le quotidien de la ville que des situations exceptionnelles ou de crise majeure.

Cette organisation repose sur une chaîne hiérarchique et opérationnelle clairement structurée. La présence d'un chef de salle, garant de la coordination opérationnelle en temps réel, devient indispensable. De même, le directeur de la police municipale doit être en mesure d'articuler finement les missions de ses équipes entre présence sur le terrain, exploitation du CSU, gestion des événements hebdomadaires et coordination étroite avec la police nationale. Cette agilité organisationnelle est au cœur du continuum de sécurité tel que défini par la loi de sécurité globale préservant les libertés.

Dans ces grandes communes, le CSU devient un véritable outil de pilotage stratégique de la sécurité et de la résilience urbaine. Il ne se limite plus à la visualisation ou à la relecture des images, mais s'inscrit dans une logique de supervision globale voire d'hypervision (gestion de la smart city), capable de soutenir la gestion d'événements de grande ampleur, de crises climatiques, de mouvements de population ou de menaces graves. La capacité à fonctionner en mode dégradé, à maintenir la continuité de service et à coordonner les acteurs du continuum constitue ici un enjeu central.



Ces collectivités disposent des moyens humains et techniques nécessaires pour structurer une exploitation avancée de la remontée de données simples à grande échelle. L'analyse des flux, des usages de l'espace public, des temporalités urbaines et des signaux faibles permet d'alimenter une stratégie de prévention, d'anticipation et d'adaptation continue des politiques publiques locales, dans le respect du cadre juridique existant et sous le contrôle du Délégué à la Protection des Données.

Enfin, les communes de plus de 100 000 habitants ont vocation à être en première ligne pour accueillir, lorsque le cadre juridique le permettra, les usages de remontée automatique d'alerte. Cette préparation ne signifie pas un déploiement anticipé, mais une capacité organisationnelle, humaine et procédurale à intégrer rapidement ces outils lorsque l'État en autorisera l'usage. À l'image de l'intégration progressive de dispositifs comme le LAPI, l'enjeu est d'être prêt à absorber ces évolutions sans rupture, dans une logique de sécurité globale, proportionnée et respectueuse des libertés publiques.

10. CE QUI PEUT RÉELLEMENT ÉVOLUER PENDANT LE MANDAT 2026-2032

10.1. IA Act, textes nationaux et travaux interministériels en cours

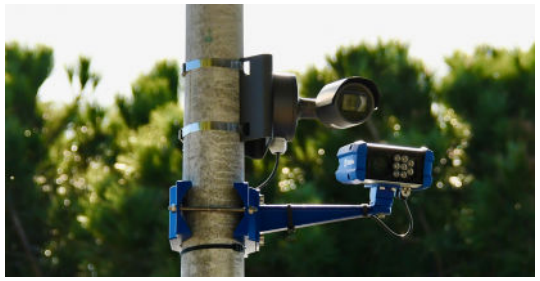
Le mandat municipal 2026–2032 s'ouvrira dans un contexte normatif en profond mouvement concernant l'usage de l'intelligence artificielle appliquée à la vidéoprotection et aux dispositifs de sécurité. En ce qui concerne l'Europe, l'IA Act EU pose désormais un cadre structurant, fondé sur une approche par les risques, qui distingue clairement les usages interdits (la reconnaissance faciale en mode nasse), les usages à haut risque soumis à des exigences renforcées, et les usages autorisés sous conditions. Ce texte ne détaille pas les modalités opérationnelles applicables aux collectivités, mais il fixe un socle commun qui s'imposera progressivement aux États membres.

En parallèle, la France a engagé un travail approfondi d'adaptation et de clarification de son droit interne. Sous l'impulsion du ministère de l'Intérieur, et notamment de la DEPSA, de la DLPAJ et des services opérationnels, une analyse croisée a été conduite à partir de plus de 200 cas d'usage recensés par l'AN2V. L'objectif est double : identifier ce qui est déployable à droit constant, ce qui nécessite un encadrement juridique spécifique, et ce qui relève clairement d'usages hors champ sécuritaire. Ces travaux constituent aujourd'hui une base de référence partagée entre juristes et opérationnels, appelée à nourrir les futures évolutions réglementaires et législatives.

Dans le même temps, le débat parlementaire s'intensifie. Députés et sénateurs multiplient les propositions de loi visant à adapter le Code de la sécurité intérieure à l'évolution des technologies, en particulier sur des sujets comme la lecture automatisée de plaques d'immatriculation ou certains usages de prévention et de maintien de l'ordre. Ces textes, parfois adoptés en procédure accélérée, traduisent moins une rupture qu'un mouvement progressif d'élargissement encadré des finalités et

des conditions d'usage, sous le contrôle du juge et avec des garanties renforcées.
Dans cette effervescence normative, le rôle de l'AN2V est déterminant. Par un travail constant de structuration, de dialogue avec les services de l'État, d'éclairage des élus et de contribution aux débats publics, l'association s'est imposée comme un acteur de référence pour dépasser les postures idéologiques et construire une vidéoprotection utile, proportionnée et juridiquement robuste.
La ténacité de l'AN2V, y compris dans le dialogue avec le Parlement, illustre une conviction forte : l'efficacité opérationnelle et le respect des libertés publiques ne s'opposent pas, ils se renforcent mutuellement.

10.2. LAPI : état des lieux, usages existants et perspectives d'ouverture
La lecture automatisée de plaques d'immatriculation constitue un exemple particulièrement éclairant de la manière dont un usage technologique peut évoluer progressivement dans le cadre juridique français, sans rupture brutale mais par ajustements successifs. Longtemps cantonnée à des finalités limitées et à un usage quasi exclusivement étatique, la LAPI illustre aujourd'hui la façon dont le législateur adapte le droit aux réalités opérationnelles, tout en maintenant des garanties fortes en matière de libertés publiques.



À ce jour, la LAPI est un outil encadré par le Code de la sécurité intérieure, principalement utilisé par les forces de sécurité de l'État à des fins de police judiciaire, de lutte contre certaines infractions graves et, plus récemment, de prévention du terrorisme. Les collectivités territoriales peuvent être associées à ces dispositifs, notamment par le financement ou l'hébergement d'infrastructures, mais l'exploitation des données demeure strictement réservée aux services de l'État, dans un cadre conventionné et contrôlé.
Les évolutions législatives récentes confirment toutefois un changement de doctrine progressif. L'adoption en première lecture par le Sénat d'une proposition de loi visant à élargir certaines finalités de la LAPI, à allonger la durée de conservation des données et à autoriser des usages temporaires en matière de maintien de l'ordre lors de grands événements traduit une inflexion nette. Sans instaurer une ouverture générale, le législateur reconnaît implicitement que la LAPI tend à devenir un outil de plus en plus transversal, à la frontière entre police judiciaire, prévention et gestion de l'ordre public.
Pour les collectivités, cette évolution appelle une lecture nuancée. D'un côté, elle confirme que des usages initialement perçus comme exceptionnels peuvent, avec le temps, être intégrés dans le droit commun, à condition d'un encadrement strict, d'un contrôle judiciaire et de garanties proportionnées. De l'autre, elle rappelle que le rôle des communes reste encadré : le principe du conventionnement facultatif est maintenu, sans obligation d'équipement, et la maîtrise des données demeure un point de vigilance majeur.
La trajectoire de la LAPI est particulièrement instructive pour les débats à venir autour de la remontée automatique d'alerte (R2A). Elle montre que l'ouverture des usages ne se fait ni par effet d'annonce, ni par généralisation immédiate, mais par une succession d'étapes, fondées sur des retours d'expérience, des arbitrages politiques et un débat parlementaire exigeant. Pour les élus locaux, l'enjeu n'est donc pas d'anticiper des usages encore hors cadre, mais de comprendre cette dynamique afin de préparer leurs organisations, leurs conventions et leurs doctrines d'emploi à des évolutions qui pourraient intervenir au cours du mandat 2026–2032.

10.3. Rôle des réseaux, référentiels et productions de l'AN2V pendant le mandat
Les évolutions juridiques et réglementaires qui encadrent les usages de la vidéoprotection et de la R2A ne se feront ni en une fois, ni de manière linéaire. Elles résulteront, comme l'illustre le cas de la LAPI, d'une succession de textes, de doctrines administratives, de décisions juridictionnelles et de retours d'expérience opérationnels. Dans ce contexte, la capacité d'une collectivité à rester à jour sans être ni en retard ni hors cadre repose avant tout sur l'accès à une information fiable, contextualisée et partagée.
Le rôle des réseaux professionnels prend ici tout son sens. L'AN2V s'est structurée précisément pour assurer cette fonction de veille, de mise en perspective et de traduction opérationnelle des évolutions en cours, au bénéfice des élus et de leurs équipes. Les travaux menés au sein des groupes de travail, les référentiels produits, ainsi que les temps d'échange organisés tout au long de l'année permettent de dépasser la lecture brute des textes pour en comprendre les implications concrètes à l'échelle des territoires.
Cette logique s'incarne notamment dans les formats de travail développés par l'AN2V, comme l'approche « 1 jour pour 5 ans » du 23 juin 2026 à Chartres, qui vise à donner en une journée une vision claire et réaliste des trajectoires possibles sur la durée d'un mandat municipal. Elle se prolonge également par l'accès à une bibliothèque de ressources, régulièrement enrichie, qui permet aux collectivités de s'appuyer sur des analyses juridiques, des retours d'expérience et des productions de référence.
Concrètement, les collectivités qui souhaitent s'inscrire dans cette dynamique peuvent simplement se signaler auprès de l'AN2V afin de recevoir les informations, convocations et invitations aux travaux et événements organisés tout au long de l'année. Ce point d'entrée permet également d'accéder aux ressources documentaires mises à disposition et de rester connecté aux évolutions du cadre juridique et opérationnel pendant toute la durée du mandat.

10.4. Les futurs grands champs d'usage de la R2A au regard du Code de la sécurité intérieure
Les débats autour de la R2A sont souvent biaisés par une vision réductrice, laissant croire qu'il s'agirait de quelques cas d'usage marginaux ou expérimentaux. Les travaux menés par l'AN2V avec les services de l'État racontent une toute autre histoire. Sans pouvoir rendre publics les résultats détaillés des enquêtes conduites auprès de la DGGN, de la DGPN, de la Préfecture de police de Paris et de la DGSCGC, les ordres de grandeur suffisent à mesurer l'enjeu : ce sont respectivement 81, 78, 50 et 42 cas d'usage identifiés comme présentant un intérêt opérationnel réel, parmi le tableau AN2V présenté de 204 idées de cas d'usages, dont une part significative est jugée prioritaire ou à fort potentiel.
Note : Les usages sélectionnés ne sont pas les mêmes ! ils sont panachés parmi le tableau de 204 usages

	DGGN	DGPN	PP	DGSCGC
	81	78	50	42
Oui niveau 5 :		12		
Oui niveau 4 :		28		
Oui niveau 3 :		9		
Oui niveau 2 :	74	14	16	
Oui niveau 1 (prioritaire) :	7	15	34	42

Ces chiffres traduisent une réalité de terrain partagée par les forces de sécurité et de secours. Ils sont issus d'un travail méthodique de recensement et de qualification de 204 cas d'usage, ensuite croisés avec les 11 finalités prévues par l'article L251-2 du Code de la sécurité intérieure. Cette approche permet de sortir du débat abstrait sur « l'IA » pour raisonner en besoins opérationnels concrets, juridiquement situés et hiérarchisés dans le temps
Les analyses convergent vers quatre grands champs d'usage structurants, qui correspondent aux finalités déjà inscrites dans le droit, ou susceptibles de l'être à court ou à moyen terme.

10.4.1. **L251-2 5°** : prévention des atteintes à la sécurité des personnes et des biens
Il s'agit du cœur historique des usages de vidéoprotection. Les travaux montrent un intérêt mar-

qué pour des capacités de détection précoce de situations anormales ou dangereuses, qu'il s'agisse d'intrusions, de comportements violents, de personnes en difficulté ou d'événements susceptibles de dégénérer rapidement. Ces usages répondent à une logique de protection immédiate et de réduction du temps de réaction, en appui des opérateurs humains et dans le cadre du continuum de sécurité. Ils concentrent une part importante des cas jugés prioritaires par les forces de sécurité.

10.4.2. **L251-2 4°** : sécurité routière et régulation des flux
La sécurité routière apparaît comme un champ d'application particulièrement structurant de la R2A. Détection de contresens, comportements à risque, congestion anormale, incidents ou accidents constituent des situations où l'alerte rapide peut prévenir des dommages graves. Ces usages intéressent fortement les services de police et de secours car ils permettent d'articuler prévention, gestion des flux et intervention rapide, en complément des dispositifs existants de signalisation et de régulation.

10.4.3. **L251-2 6°, 7°, 8°** : risques naturels, technologiques et secours aux personnes
Les travaux menés avec la DGSCGC mettent en évidence un potentiel important dans le champ de la résilience des territoires. Détection de départs de feu, de fumées anormales, de montées des eaux, de situations météorologiques critiques ou de personnes en détresse s'inscrivent directement dans les objectifs nationaux de protection civile et de gestion de crise. Ces usages prennent une importance croissante dans un contexte de changement climatique et de multiplication des événements extrêmes, et s'inscrivent pleinement dans la stratégie nationale de résilience portée par l'État (SGDSN).

10.4.4. **L251-2 9°, 10°, 11°** : environnement, atteintes au cadre de vie et catégories résiduelles
Enfin, un ensemble plus hétérogène d'usages concerne la protection de l'environnement et du cadre de vie. Dépôts sauvages, atteintes aux équipements publics, pollutions visibles ou dégradations répétées sont autant de situations où la remontée d'alerte peut contribuer à une action plus rapide et plus ciblée. Ces usages, souvent perçus comme secondaires, sont pourtant fortement plébiscités par les collectivités car ils répondent à des problématiques très concrètes de qualité de vie et d'acceptabilité locale des dispositifs.
Pris dans leur ensemble, ces quatre champs montrent que la R2A ne se limite ni à un outil de sécurité spectaculaire, ni à un débat idéologique. Elle correspond à une demande opérationnelle large, structurée et déjà largement analysée, qui appelle désormais des arbitrages juridiques et politiques progressifs plutôt qu'une opposition de principe.

11. ORGANISATION, RESSOURCES HUMAINES ET CONDUITE DU CHANGEMENT

11.1. Passer d'un CSU de «visionnage» à un CSU «piloté par les alertes» : stratégie de «l'écran noir»

Pendant longtemps, les centres de supervision urbains ont été conçus comme des espaces de visionnage continu, accumulant les écrans et les flux vidéo dans l'idée que « voir plus » permettrait de mieux protéger. L'expérience opérationnelle montre pourtant les limites de ce modèle. L'affichage simultané de dizaines de flux, parfois jusqu'à plusieurs dizaines d'images sur de grands murs d'écrans, crée une surcharge visuelle contre-productive. Le regard humain ne peut pas rester concentré durablement sur un tel volume d'informations, et l'attention est naturellement attirée par certains éléments au détriment d'autres, au risque de manquer un événement réellement significatif.
La logique de «l'écran noir» repose sur un principe inverse. En situation nominale, les écrans n'affichent aucune image, ou seulement des informations synthétiques. Ils sont réservés à l'affichage automatique et contextuel des images lorsqu'un événement est détecté, signalé ou qualifié, qu'il s'agisse d'une alerte automatisée R2A, d'un signalement humain ou d'un appel externe. Le contraste visuel créé par l'apparition soudaine d'images sur un écran habituellement neutre permet une captation immédiate de l'attention de l'opérateur et une réaction plus rapide.
Cette approche ne vise pas à supprimer la supervision humaine, mais à la rendre plus efficace. Elle permet de concentrer l'attention sur l'essentiel, de réduire la fatigue cognitive et de travailler à partir d'événements qualifiés plutôt que d'un flux continu d'images sans information. Elle constitue le socle d'un CSU moderne, capable de passer progressivement d'un modèle de visionnage passif à un modèle piloté par les alertes et les situations à traiter.

11.2. Rôle des opérateurs et évolution des compétences

La transformation du CSU implique une évolution profonde du rôle des opérateurs. Leur mission ne consiste plus principalement à « regarder des écrans », mais à analyser des situations, qualifier des événements, déclencher des procédures et transmettre une information fiable et contextualisée aux bons interlocuteurs. Moins d'écrans visibles ne signifie pas moins de travail, mais un travail différent, plus exigeant en termes de discernement et de responsabilité.
Dans ce modèle, les opérateurs s'appuient sur des procédures formalisées et des fiches réflexes préétablies. Ces outils, construits en amont avec les services concernés (internes et/ou externes), permettent de sécuriser les décisions, d'harmoniser les pratiques et de réduire le temps de réaction. Lorsqu'une alerte survient, l'opérateur n'improvise pas : il suit un cadre clair, tout en conservant la capacité d'adaptation nécessaire à chaque situation.
Cette évolution suppose un investissement accru dans la formation et l'accompagnement des équipes. Les compétences attendues dépassent la simple maîtrise technique des outils. Elles incluent la capacité d'analyse, la gestion du stress, la compréhension des chaînes décisionnelles et la connaissance fine des partenaires du continuum de sécurité. L'opérateur devient un acteur central de la chaîne de protection et de résilience du territoire, dont la valeur repose avant tout sur la qualité du jugement et de l'interprétation, bien plus que sur le nombre d'images affichées.

11.3. Organisation des procédures, fiches réflexes et chaînes décisionnelles

La création ou la transformation d'un CSU en un outil réellement opérationnel ne repose pas uniquement sur les interfaces ou les technologies déployées, mais sur la qualité de l'organisation des procédures et des chaînes décisionnelles. Dans un modèle piloté par les alertes, les écrans noirs et le mur d'image ne prennent leur sens que s'ils sont adossés à des scénarios d'usage clairement définis, testés et régulièrement mis à jour.
L'expérience montre que les murs d'images historiquement conçus comme des mosaïques permanentes de flux vidéo atteignent rapidement leurs limites. Au-delà d'un nombre restreint d'images affichées simultanément, la capacité de perception de l'opérateur diminue fortement, et l'attention se concentre sur quelques écrans secondaires (son ordinateur) au détriment du mur principal. À l'inverse, les dispositifs modernes s'orientent vers un affichage contextuel et dynamique, dans lequel le mur d'image reste neutre en situation nominale et ne se reconfigure que lorsqu'un événement significatif survient.



Dans ce cadre, chaque type d'événement doit être associé à une procédure formalisée et à une fiche réflexe préétablie. Lorsqu'une alerte est déclenchée ou qu'un signalement est reçu, le mur d'image bascule automatiquement vers une configuration adaptée : affichage prioritaire de la caméra concernée, vues périphériques, cartographie de la zone, positionnement des

équipes disponibles et informations contextuelles utiles à la décision. L'opérateur dispose ainsi, en un coup d'œil, de l'ensemble des éléments nécessaires pour qualifier la situation, appliquer la procédure et transmettre l'information aux acteurs compétents affichés automatiquement à l'écran !
Cette organisation suppose également une articulation fluide entre les outils. Les mains courantes, appels téléphoniques, messages radio ou alertes doivent pouvoir être intégrés dans un même environnement de travail, avec des fonctions de transcription automatique ou de synthèse, afin de limiter les ruptures d'attention et les pertes d'information. Le mur d'image devient alors un véritable tableau de bord décisionnel, et non un simple support de visualisation.
Enfin, la robustesse du dispositif repose sur la clarté des chaînes décisionnelles. Chaque fiche réflexe doit préciser qui agit, qui décide, qui informe, dans quels délais, les plans B si A est absent etc. Cette structuration sécurise juridiquement les opérateurs, fluidifie les échanges avec les forces de sécurité et de secours, et permet une montée en compétence progressive des équipes. Elle doit être régulièrement réévaluée, à la lumière des retours d'expérience, afin d'affiner les scénarios, les priorités d'affichage et les procédures associées.

11.4. Articulation entre élus, directions et services : clarifier le «qui fait quoi»
La performance d'un dispositif de vidéoprotection et de supervision ne dépend pas uniquement de la qualité des outils ou des opérateurs en salle. Elle repose avant tout sur une articulation claire et assumée entre les élus et l'ensemble des directions et services concernés. Lorsque les responsabilités sont mal définies, les décisions ralentissent, les risques juridiques augmentent et les situations de crise deviennent plus difficiles à gérer.
Dans ce cadre, le rôle des élus est d'abord politique et stratégique. Ils fixent les orientations, arbitrent les priorités et assument la responsabilité des choix structurants, notamment en matière d'objectifs, de périmètre et de niveau d'ambition du dispositif. Le Directeur général des services joue un rôle central de coordination et de pilotage transversal. Il veille à la cohérence d'ensemble, à l'alignement des directions et à la bonne traduction des orientations politiques dans l'organisation opérationnelle.



La Direction des systèmes d'information intervient sur les architectures techniques, la cybersécurité, l'interopérabilité des outils et la continuité de service. Elle est un acteur clé de la robustesse du dispositif, notamment en situation dégradée. Le Délégué à la protection des données, quant à lui, garantit la conformité juridique et le respect des principes de proportionnalité, de finalité et de transparence. Son intervention en amont sécurise les décisions et protège durablement la collectivité.
La police municipale et les opérateurs du CSU constituent le cœur opérationnel du dispositif. Ils assurent la supervision, l'analyse des situations, l'application des procédures et l'articulation avec les forces de sécurité intérieure et les services de secours. Les services techniques, enfin, garantissent le maintien en condition opérationnelle des équipements, la réactivité en cas de panne et la qualité des infrastructures. Les services de communication jouent un rôle complémentaire mais essentiel, en assurant l'information du public et la pédagogie autour des dispositifs déployés.
Pour éviter les zones grises et les décisions implicites, de nombreuses collectivités s'appuient sur une méthode simple et éprouvée : le RACI. Cette approche consiste à définir, pour chaque processus ou situation, qui est Responsable de l'action, qui en est l'Approbateur, qui doit être Consulté et qui doit être Informé. Sans entrer dans une logique bureaucratique, le RACI permet de sécuriser les décisions, d'accélérer les réactions et de clarifier les responsabilités, en particulier dans les situations sensibles ou de crise.

12. ENCADREMENT ÉTHIQUE, MAÎTRISE DES RISQUES ET ACCEPTABILITÉ DÉMOCRATIQUE

L'acceptabilité des dispositifs de vidéoprotection et de leurs évolutions ne se décrète pas. Elle se construit dans la durée, par des choix de gouvernance clairs, une transparence assumée et une capacité à traiter les risques réels sans posture défensive. Dans un contexte de débats parfois très polarisés, l'enjeu pour les collectivités n'est pas de convaincre à tout prix, mais de démontrer leur capacité à décider de manière responsable, proportionnée et contrôlable.
12.1. L'intérêt d'un comité d'éthique local pour sécuriser les décisions
Plusieurs grandes collectivités ont fait le choix, depuis de nombreuses années, de se doter d'un comité ou d'un collège d'éthique dédié aux usages de la vidéoprotection. La ville de Lyon a été l'une des premières à ouvrir cette voie, bien avant que ces sujets ne deviennent centraux dans le débat public. Cette démarche ne relève pas d'un affichage, mais d'un outil de gouvernance à part entière.
Un comité d'éthique local permet d'instaurer un espace de régulation déontologique, indépendant des décisions opérationnelles quotidiennes. Il joue un rôle d'avis et de proposition sur les projets, les évolutions d'usage et les conditions d'exploitation du dispositif. Sa composition doit répondre à des objectifs d'équilibre, de pluralité et d'indépendance, en associant des représentants de la collectivité, des communes membres le cas échéant, et des personnalités qualifiées ou représentants de la société civile.
L'existence d'un tel comité ne ralentit pas l'action publique. Au contraire, elle sécurise les décisions politiques et administratives en amont, en permettant d'identifier les points de vigilance avant qu'ils ne deviennent des sujets de controverse ou de contentieux.

12.2. Les risques réels : biais, dépendance industrielle, dérives d'usage, opacité
Les débats sur la vidéoprotection et les outils d'analyse sont souvent alimentés par des risques théoriques ou fantasmés. Cela ne doit pas conduire à minimiser les risques réels, qui existent et doivent être traités avec sérieux. Parmi eux figurent les biais potentiels dans les outils, la dépendance à des solutions industrielles peu transparentes (contexte géopolitique tendu), les dérives d'usage liées à une extension progressive des finalités, ou encore l'opacité perçue par les citoyens.
La réponse à ces risques ne réside pas dans des discours généraux, mais dans une doctrine d'emploi claire. Une charte éthique constitue à cet égard un outil structurant. Son principe peut se résumer simplement : « dire ce que l'on fait, et faire ce que l'on dit ». Elle explicite les finalités poursuivies, les usages exclus, les règles de visualisation, de relecture et d'extraction des images, ainsi que les conditions dans lesquelles les opérateurs doivent être en mesure de justifier leurs actions, y compris devant l'autorité judiciaire, ou après l'usage d'un droit à l'image d'un citoyen.

12.3. Les leviers de prévention : gouvernance, contrats, audits et réversibilité
La maîtrise des risques passe d'abord par la gouvernance. La clarification des rôles, l'implication du Délégué à la Protection des Données (DPD), la traçabilité des décisions et l'existence d'instances de suivi constituent des leviers essentiels. À cela s'ajoutent des choix contractuels structurants : clauses de réversibilité, exigences d'interopérabilité, limitation des dépendances technologiques et capacité à auditer les solutions déployées.
Les audits, qu'ils soient juridiques, organisationnels ou techniques, doivent être envisagés comme des outils de pilotage et non comme des sanctions. Ils permettent d'objectiver les pratiques, d'identifier les écarts éventuels et d'ajuster les dispositifs dans le temps. Cette approche pragmatique renforce la robustesse du système et la confiance des parties prenantes.

12.4. Auditabilité et traçabilité des algorithmes sans entrer dans la boîte noire

La question de l'auditabilité des outils, notamment lorsqu'ils intègrent des traitements automatisés (R2A ou R2D), est centrale. Il ne s'agit pas pour une collectivité de comprendre ou d'expliquer le fonctionnement interne de chaque algorithme, mais d'être en mesure de démontrer comment et dans quelles conditions une alerte ou une information a été produite.

La traçabilité des actions, des accès et des décisions constitue à cet égard un prérequis. Elle participe à la souveraineté de la collectivité sur ses dispositifs et permet de dire les choses clairement aux citoyens : ce qui est fait, ce qui ne l'est pas, et comment les contrôles sont exercés. Cette transparence factuelle est souvent plus efficace que de longs discours techniques.

12.5. Construire un récit public centré sur la prévention, le secours et la résilience

L'acceptabilité démocratique repose aussi sur le récit public porté par la collectivité. Lorsque la vidéoprotection est présentée exclusivement sous l'angle répressif ou sécuritaire, elle cristallise les oppositions. À l'inverse, un discours centré sur la prévention, la protection des personnes, le secours et la résilience des territoires permet de reconnecter ces dispositifs à des préoccupations concrètes et partagées.

Ce récit doit s'appuyer sur des faits, des chiffres, des retours d'expérience et des exemples d'usages utiles. Il doit également reconnaître les limites et les garde-fous, sans chercher à les minimiser. Cette posture de transparence renforce la crédibilité de la collectivité et la confiance des habitants.

12.6. Répondre aux controverses et aux oppositions sans confrontation stérile

Les controverses autour de la vidéoprotection et de ses évolutions ne relèvent pas uniquement d'un désaccord idéologique. Elles traduisent souvent une défiance plus large vis-à-vis de la décision publique, nourrie par un sentiment d'opacité ou de décisions perçues comme imposées. Y répondre efficacement suppose de déplacer le débat du terrain de la conviction vers celui de la compréhension et de la confiance.

Les collectivités qui parviennent à apaiser durablement ces oppositions ne sont pas celles qui cherchent à convaincre à tout prix, mais celles qui assument une transparence active. Expliquer clairement les objectifs poursuivis, les limites assumées et les garde-fous mis en place permet de sortir d'un face-à-face idéologique et de réinscrire le débat dans un cadre rationnel. Informer ne consiste pas à multiplier les discours, mais à rendre lisible ce qui est fait, pourquoi cela est fait et dans quelles conditions.

Cette démarche gagne en crédibilité lorsqu'elle s'appuie sur des éléments objectivés. Les enquêtes récentes montrent que la vidéoprotection et certains usages encadrés de la R2D ou R2A sont aujourd'hui largement perçus comme des outils utiles, tant par les citoyens que par les élus. Ce constat ne vaut pas adhésion inconditionnelle, mais il rappelle une réalité essentielle : le débat ne se joue plus entre rejet massif et adhésion aveugle, mais autour des conditions de gouvernance, de transparence et de respect des libertés publiques.

Dans ce contexte, la posture la plus robuste consiste à reconnaître explicitement les points de vigilance plutôt qu'à les minimiser. Libertés publiques, cadre juridique, gouvernance des données, coût et utilité réelle doivent être abordés frontalement. C'est précisément cette capacité à dire ce qui est interdit autant que ce qui est autorisé qui permet de construire un climat de confiance et de désamorcer les oppositions les plus durables.

Certaines collectivités ont fait le choix d'ouvrir ponctuellement leurs dispositifs au regard citoyen, via des réunions publiques, des travaux de comités d'éthique ou des visites encadrées de centres de supervision. Lorsqu'elles sont maîtrisées, ces démarches contribuent à démystifier les dispositifs, à montrer la place centrale de l'humain dans la décision et à rappeler que la vidéoprotection n'est ni autonome ni incontrôlable.

Répondre aux oppositions ne signifie pas rechercher l'unanimité, mais démontrer une capacité à gouverner avec méthode, clarté et responsabilité. Dans un débat souvent polarisé, cette posture constitue moins un risque politique qu'un facteur de crédibilité durable sur l'ensemble du mandat.

PARTICIPEZ À L'ÉVÉNEMENT AN2V DE LA SÛRETÉ 2026

Bâtissons ensemble les stratégies de sécurité de demain

1 JOUR POUR 5 ANS
23 JUIN 2026
CHARTRES



Le **23 juin 2026**, à Chartres, l'AN2V organise une journée exceptionnelle : **1 Jour pour 5 Ans**. Un rendez-vous unique qui rassemble les décideurs publics, privés ouverts aux publics et privés, venus bâtir les stratégies de sécurité de demain.

Découvrez des IDÉES DÉDIÉES sur les stands des exposants

Participez aux ATELIERS COLLABORATIFS thématiques avec vos pairs.

1000 DÉCIDEURS attendus pour un rendez-vous exceptionnel.

75 TABLES x 3 IDÉES = 225 IDÉES
POUR TRANSFORMER LA SÉCURITÉ DE DEMAIN

ACCÈS GRATUIT POUR LES UTILISATEURS FINAUX

VIDÉOPROTECTION

PARTIE 3 : DÉCIDER, ARBITRER ET ASSUMER SUR LE MANDAT

LECTURE RAPIDE : DÉCIDER, ARBITRER ET ASSUMER SUR LE MANDAT MUNICIPAL

LA TROISIÈME PARTIE DU LIVRE BLANC S'ADRESSE AUX ÉLUS QUI ONT DÉPASSÉ LE STADE DE LA RÉFLEXION ET DOIVENT DÉSORMAIS INSCRIRE LEURS CHOIX DANS UNE TRAJECTOIRE POLITIQUE CRÉDIBLE, JURIDIQUEMENT SÉCURISÉE ET OPÉRATIONNELLEMENT SOUTENABLE. ELLE TRAITE MOINS DE TECHNOLOGIES QUE DE GOUVERNANCE, DE TEMPORALITÉ ET DE RESPONSABILITÉ SUR L'ENSEMBLE DU MANDAT MUNICIPAL.

Le chapitre 13 invite les élus à raisonner en trajectoire plutôt qu'en annonces. Il rappelle qu'un mandat municipal se déploie en plusieurs temps, chacun appelant des décisions différentes. Les premiers mois doivent être consacrés à l'audit, à la clarification des usages existants et à la définition d'une doctrine d'emploi, plutôt qu'à des déploiements visibles mais fragiles. Le cœur du mandat permet ensuite des évolutions maîtrisées, fondées sur des organisations stabilisées et des choix assumés. Enfin, la fin du mandat impose une vigilance particulière pour éviter les décisions précipitées ou symboliques, souvent sources de fragilité politique et juridique. Ce chapitre aide les élus à comprendre que la crédibilité se construit dans la cohérence et la continuité, non dans la rupture.

Le chapitre 14 adapte cette réflexion à la réalité des territoires. Il montre que les marges de manœuvre, les risques et les priorités ne sont pas les mêmes selon la taille de la collectivité. Petites communes, villes moyennes ou grandes agglomérations n'ont ni les mêmes moyens humains, ni les mêmes niveaux d'exposition, ni les mêmes capacités de gouvernance. Ce chapitre aide à éviter les comparaisons artificielles et les modèles importés, en invitant chaque élu à construire une stratégie proportionnée et adaptée à son contexte local.

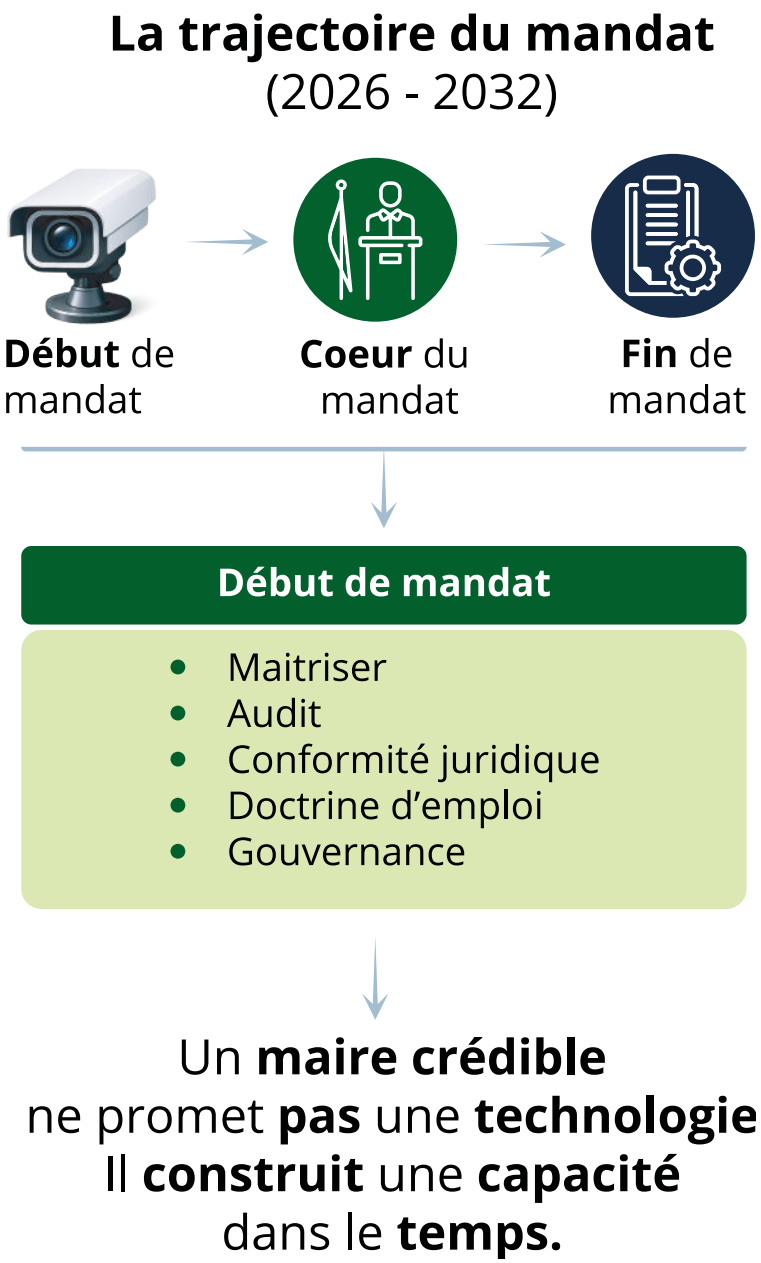
Le chapitre 15 aborde les choix administratifs et contractuels qui sécurisent ou fragilisent durablement un projet. Il rappelle qu'un dispositif de vidéoprotection ou d'évolution vers de nouveaux usages devient rapidement un marché public structurant, engageant la collectivité sur plusieurs années. Les points de vigilance contractuels, la réversibilité, la dépendance industrielle, la maintenance et l'intégration des contraintes réglementaires doivent être anticipés dès la conception. Ce chapitre montre que les décisions techniques mal cadrées deviennent très vite des problèmes politiques difficiles à corriger.

Le chapitre 16 élargit enfin la réflexion aux conditions de pilotage dans la durée. Il insiste sur la nécessité de documenter les décisions, de tracer les usages, de sécuriser juridiquement les arbitrages et de maintenir une capacité d'adaptation face aux évolutions réglementaires, technologiques et sociétales. Ce chapitre rappelle que gouverner un dispositif dans le temps est aussi important que le décider, et que la maîtrise du cadre éthique, juridique et organisationnel constitue la meilleure protection pour les élus.

DANS SON ENSEMBLE, CETTE TROISIÈME PARTIE VISE À AIDER LES MAIRES ET LEURS ÉQUIPES À PASSER D'UNE LOGIQUE DE PROJET À UNE LOGIQUE DE RESPONSABILITÉ POLITIQUE. ELLE MONTRE QUE LA VIDÉOPROTECTION ET SES ÉVOLUTIONS POSSIBLES NE SONT NI DES SUJETS TECHNIQUES ISOLÉS NI DES RÉPONSES IMMÉDIATES, MAIS DES CHOIX STRUCTURANTS QUI ENGAGENT LA COLLECTIVITÉ SUR LA DURÉE DU MANDAT ET AU-DELÀ.

13. CONSTRUIRE UNE TRAJECTOIRE POLITIQUE CRÉDIBLE SUR LE MANDAT 2026-2032

Les choix en matière de vidéoprotection, de CSU et d'évolutions possibles vers des usages de type R2A ne peuvent pas être traités comme un projet technique isolé. Ils engagent la responsabilité politique du maire sur la durée du mandat, exposent la collectivité à des risques juridiques et médiatiques, et structurent durablement l'organisation municipale. La crédibilité ne se joue donc ni dans l'annonce, ni dans la rupture, mais dans la trajectoire.
Un mandat municipal se déploie en plusieurs temps. Chacun appelle des décisions différentes, non seulement en termes d'équipement, mais surtout de gouvernance, d'organisation et de discours public. Assumer cette temporalité est la meilleure protection contre les promesses intenables et les procès d'intention.



13.1. Les six premiers mois

Les six premiers mois du mandat constituent un moment politique singulier. Les attentes sont fortes, les oppositions attentives, et les marges de manœuvre encore réelles. C'est pourtant le pire moment pour annoncer des déploiements technologiques ambitieux. Le signal crédible attendu n'est pas celui de la nouveauté, mais celui de la maîtrise.
Cette première phase doit être consacrée à un travail de fond souvent invisible mais déterminant : audit de l'existant, analyse des usages réels, évaluation de la conformité juridique, état des lieux des organisations humaines et clarification des relations avec les services de l'État. Elle permet de distinguer ce qui fonctionne de ce qui relève de l'affichage, et de sortir des idées reçues sur l'efficacité ou le coût de la vidéoprotection.
C'est également le bon moment pour fixer publiquement une doctrine d'emploi. Dire ce que la commune fait déjà, ce qu'elle entend améliorer, et surtout ce qu'elle ne fera pas à ce stade permet de reprendre la main sur le récit. L'annonce de la mise en place d'instances de gouvernance, comme un comité d'éthique ou des engagements de transparence, constitue un signal politique fort, sans exposer la collectivité à des risques prématurés.

13.2. Le cœur du mandat

Le cœur du mandat est le temps de la consolidation et de la mise en œuvre. C'est à ce moment-là que les choix posés en début de mandat prennent corps et que la crédibilité politique du projet se construit dans la durée. Contrairement aux idées reçues, l'efficacité réelle des dispositifs ne se joue ni dans l'annonce initiale, ni dans l'empilement rapide de technologies, mais dans la capacité à déployer progressivement ce qui a été pensé, documenté et assumé.
Cette phase correspond au déploiement maîtrisé du schéma directeur arrêté en début de mandat. Elle peut inclure, lorsque cela est justifié, l'extension du parc de caméras, l'amélioration des infrastructures réseau, la montée en capacité des centres de supervision et le renforcement des moyens humains. L'enjeu n'est pas de faire plus, mais de faire juste, en cohérence avec les objectifs identifiés et les moyens réellement disponibles.
C'est également au cours de cette période que les usages de remontée de données simples peuvent être pleinement structurés. L'exploitation raisonnée de données statistiques et agrégées, à des fins de gestion du territoire, permet d'objectiver les décisions publiques, d'éclairer les politiques locales et d'améliorer l'efficacité opérationnelle, sans entrer dans des usages juridiquement fragiles. Cette logique constitue le socle naturel de la montée en compétence des équipes et de la valeur produite par le dispositif.
La question des usages de remontée automatique d'alerte peut également se poser durant le cœur du mandat, mais dépendra de l'éventuelle évolutions du cadre juridique national et européen. Cela implique une veille réglementaire et législative continue, menée avec rigueur, mois après mois, afin de distinguer ce qui relève d'une ouverture réelle du droit de ce qui n'est encore qu'un débat ou une expérimentation. En aucun cas ces usages ne doivent être promis ou engagés par anticipation.
Cette montée en puissance progressive apporte une réponse directe aux critiques récurrentes sur le coût, l'inefficacité ou le caractère liberticide de la vidéoprotection. L'efficacité ne réside pas dans la sophistication technologique, mais dans la capacité à agir plus vite, à mieux coordonner les acteurs et à réduire les angles morts organisationnels. En restant strictement dans le cadre juridique existant, en documentant les résultats et en ajustant les dispositifs en fonction des usages réels, la collectivité se place sur un terrain factuel, pragmatique et difficilement contestable.

13.3. La fin du mandat

La fin du mandat ne doit pas être le temps de l'accélération artificielle. C'est au contraire celui de la transmission. Une collectivité responsable prépare l'équipe suivante en lui laissant une situation lisible, documentée et évolutive, plutôt qu'un empilement de dispositifs difficilement gouvernables. Préparer l'héritage du mandat consiste à formaliser les doctrines d'emploi, stabiliser les organisations, consolider les outils de gouvernance et expliciter les limites assumées. Cela inclut le fait de ne pas avoir déployé certains usages tant que le cadre juridique ne le permettait pas, et de l'avoir

expliqué clairement aux habitants.
Cette posture est politiquement exigeante, mais elle constitue la meilleure réponse aux accusations de dérive sécuritaire ou de surveillance généralisée. Une collectivité qui transmet des règles claires, des contrôles effectifs et une organisation robuste démontre que la vidéoprotection est un service public encadré, réversible et démocratiquement contrôlé, et non un instrument de pouvoir.

14. ADAPTER SA STRATÉGIE… ET ÉVITER LES ERREURS CLASSIQUES SELON LA TAILLE DE LA COLLECTIVITÉ

Il n'existe pas de modèle unique en matière de vidéoprotection, de CSU ou d'évolutions possibles vers des usages de type R2A. Les stratégies pertinentes dépendent étroitement de la taille de la collectivité, de son organisation administrative, de ses moyens humains et de son contexte territorial. Les erreurs les plus fréquentes ne tiennent pas à de mauvaises intentions, mais à des raisonnements par mimétisme ou à des projections irréalistes.

14.1. Petites communes

La première erreur des petites communes consiste à vouloir reproduire des modèles conçus pour des villes beaucoup plus importantes. Copier l'architecture, les équipements ou les discours de grandes collectivités conduit presque systématiquement à des dispositifs sous-exploités, coûteux et politiquement fragiles. L'enjeu principal n'est pas technologique mais organisationnel.
Promettre du temps réel en continu sur l'espace public sans disposer d'opérateurs dédiés, d'une organisation h24 et de procédures stabilisées expose la commune à des critiques immédiates et légitimes. De la même manière, évoquer des alertes automatiques ou des capacités d'intervention sans chaîne opérationnelle claire crée des attentes irréalistes et juridiquement fragiles.
Il convient toutefois de nuancer ce constat selon les espaces concernés. Le temps réel est parfaitement envisageable, et souvent pertinent, au sein des bâtiments communaux lorsque ceux-ci sont fermés. Pour une école, une mairie annexe ou un équipement sportif, la nuit, le week-end ou pendant les vacances scolaires, l'activation d'une alarme peut déclencher une réponse immédiate structurée, confiée à une société de sécurité privée. La chaîne opérationnelle est alors claire et maîtrisée : détection de l'événement, transmission de l'information, levée de doute par la visualisation, puis intervention sur site. Ce type d'organisation, fondé sur des espaces privés ou strictement maîtrisés, est à la fois légal, efficace et proportionné.
En revanche, cette logique de temps réel sur l'espace public ou dans les espaces privés ouverts au public ne peut fonctionner que dans le cadre de centres de supervision organisés en continu. Sans CSU h24, il est illusoire de promettre le même niveau de réactivité. C'est précisément pour cette raison que les petites communes ont tout intérêt à explorer des formes de mutualisation, qu'il s'agisse d'un CSUi porté par le bloc communal ou d'un centre départemental de supervision, afin d'accéder, le cas échéant, à une capacité de temps réel sur l'espace public qu'elles ne peuvent assumer seules.
Pour ces communes, la stratégie raisonnable repose donc sur la proportionnalité et la complémentarité. Sécuriser les bâtiments communaux en temps réel lorsqu'ils sont fermés, exploiter les images à des fins d'élucidation et de prévention situationnelle sur l'espace public, et s'inscrire dans des coopérations structurées constituent des choix défendables et efficaces.

14.2. Villes moyennes

Dans les villes moyennes, la question centrale n'est pas le nombre d'habitants, mais la capacité de la collectivité à structurer une exploitation humaine du dispositif de vidéoprotection. Tant qu'aucun opérateur n'est dédié à la supervision, la commune se situe, de fait, dans une logique proche de celle des petites collectivités, même si un centre de supervision existe physiquement. Sans présence humaine organisée, un CSU reste un outil de consultation différée, et non un levier de réaction en temps réel.
Le véritable point de bascule intervient avec l'embauche progressive d'opérateurs. La présence de deux ou trois agents permet déjà d'écrêter les périodes les plus sensibles de la vie locale : événements festifs, pics d'affluence saisonniers, soirées de week-end, fêtes nationales ou situations récurrentes de tension. À ce stade, la commune peut commencer à tenir une promesse crédible de réaction en temps réel sur des plages ciblées, à condition que les procédures et les chaînes de transmission soient clairement définies.
Cette première montée en charge ouvre également la possibilité d'introduire de manière limitée certains usages de remontée automatique d'alerte (R2A), lorsque le cadre juridique le permet, en appui direct des opérateurs présents en salle. L'enjeu n'est pas la généralisation, mais l'apprentissage progressif, la montée en compétence des équipes et la stabilisation des processus.
Pour atteindre un fonctionnement réellement continu, les ordres de grandeur sont bien connus. Il faut environ sept opérateurs pour assurer une présence h24 365j/an avec un agent en salle, une dizaine pour organiser des rotations plus confortables, et une quinzaine pour garantir, statistiquement, la présence de deux opérateurs en permanence. Ces volumes dépassent souvent les capacités d'une seule ville moyenne, ce qui rend la question de la mutualisation incontournable.
C'est pourquoi, pour ces collectivités, la stratégie pertinente consiste à raisonner à l'échelle du territoire plutôt qu'à celle du seul périmètre communal. Mutualiser un CSU avec des communes voisines, s'inscrire dans un CSUi ou s'appuyer sur un dispositif départemental permet d'atteindre une capacité de temps réel et d'ouvrir progressivement la voie à des usages plus avancés, sans fragiliser l'organisation ni les finances locales.

14.3. Grandes villes et métropoles

Dans les grandes villes et les métropoles, la question n'est plus celle de l'accès au temps réel, mais celle de sa maîtrise dans la durée. Ces collectivités disposent en général des moyens humains suffisants pour structurer un CSU actif, fonctionnant en continu, avec des équipes dimensionnées pour assurer une présence permanente, souvent avec plusieurs opérateurs simultanément. À ce stade, le temps réel n'est plus une ambition, mais une réalité opérationnelle quotidienne.
Le principal risque pour ces collectivités n'est donc pas le sous-dimensionnement, mais la complexité mal gouvernée. L'augmentation du nombre de caméras et la gestion du parc, la diversification des usages, la multiplication des alertes potentielles et la segmentation des territoires peuvent rapidement conduire à une surcharge informationnelle, à une fatigue des opérateurs et à une perte de lisibilité des priorités. Plus la capacité humaine augmente, plus la nécessité d'un pilotage rigoureux devient critique.

Ce qui est raisonnable selon la taille de collectivité.

Taille	Temps réel	Stratégie raisonnable
Petite Commune	✘ Non hors mutualisation	Espace non ouvert au public + différé
Ville moyenne	○ Ciblé	Temps réel ciblé
Grande Ville Métropole	✔ Oui	Priorisation + gouvernance

Le vrai seuil n'est pas démographique, il est dépendant des ressources.

Dans ce contexte, l'introduction d'usages de type R2A doit être pensée comme un outil d'aide à la décision et de priorisation, jamais comme un substitut à l'analyse humaine. Les grandes collectivités sont les mieux placées pour expérimenter, lorsque le cadre juridique le permet, des dispositifs plus avancés, à condition de les inscrire dans des procédures robustes, des chaînes décisionnelles claires et une gouvernance éthique assumée. La performance ne vient pas de la sophistication maximale, mais de la capacité à filtrer, qualifier, hiérarchiser et traiter efficacement les situations réellement pertinentes.
Enfin, ces collectivités doivent intégrer très tôt les enjeux de résilience globale. Continuité énergétique, cybersécurité, fonctionnement en mode dégradé et articulation avec les forces de sécurité intérieure et les services de secours sont des prérequis indispensables. À ce niveau de complexité, un CSU n'est plus seulement un outil de sécurité, mais un véritable centre de pilotage territorial, au cœur du continuum de sécurité.

14.4. Attention à la bonne définition des coopérations

La mutualisation est souvent présentée comme une réponse évidente aux contraintes budgétaires et organisationnelles. En pratique, elle n'est efficace que si elle repose sur des conventions claires, réalistes et politiquement assumées. Les difficultés apparaissent dès lors que la coopération est pensée uniquement sous l'angle technique, sans alignement préalable sur les capacités humaines disponibles, les niveaux de service attendus, ni sur la répartition des responsabilités juridiques, financières et opérationnelles.
Les écueils les plus fréquents tiennent à des périmètres mal définis, à des conventions imprécises ou à des attentes asymétriques entre collectivités. Une commune qui s'inscrit dans un dispositif mutualisé sans disposer elle-même d'une organisation minimale peut attendre du CSU partagé des capacités qu'il n'est pas en mesure de fournir. À l'inverse, une collectivité support peut se retrouver à assumer des charges opérationnelles, financières et politiques qu'elle n'avait ni anticipées ni acceptées explicitement.
Une coopération réussie repose donc avant tout sur une clarification des rôles et des engagements. Qui assure la supervision en temps réel, sur quels horaires, avec quels effectifs, pour quels types d'événements, selon quelles procédures et avec quelles limites ? Ces questions doivent être tranchées en amont, formalisées dans des conventions robustes et potentiellement réévaluées dans le temps. La mutualisation n'est pas une délégation de responsabilité, mais un partage organisé de capacités clairement définies.
Lorsqu'elle est bien pensée, la mutualisation permet d'atteindre des seuils humains autrement inaccessibles, notamment pour assurer une présence h24 365j/an, renforcer la résilience du territoire et, le cas échéant, ouvrir l'accès à des usages de temps réel sur l'espace public. Là encore, la clé n'est ni la technologie ni la taille des collectivités, mais la cohérence entre ambitions, moyens humains et gouvernance territoriale.

Une convention de mutualisation doit décrire de manière explicite les services réellement rendus. À titre indicatif, et selon le niveau d'organisation retenu, ceux-ci peuvent inclure :

- Assistance à la visualisation et à l'analyse des événements significatifs, en appui ou en renfort des équipes locales lorsqu'elles existent.
- Protection des sites et équipements sur des plages horaires étendues, pouvant aller jusqu'au 24h/24 et 7j/7 lorsque l'organisation humaine le permet.
- Détection et qualification d'événements anormaux ou atypiques, dans les limites du cadre juridique applicable.
- Appui à la protection des interventions humaines sur site, de jour comme de nuit.
- Maintien en condition opérationnelle du dispositif : supervision technique, sécurisation des enregistrements, détection des pannes et gestion des incidents.
- Capacité de réaction rapide et coordonnée face aux situations critiques, dans un cadre procédural partagé.
- Mise en place d'un socle de confiance en matière de cybersécurité et de protection des infrastructures.
- Garanties opérationnelles de conformité RGPD, en lien avec les DPO/DPD des collectivités concernées.
- Facilitation du travail des forces de sécurité intérieure, notamment par la capacité à visualiser et exploiter des images issues de plusieurs communes depuis un point centralisé, dans un cadre strictement encadré.

Pour structurer efficacement ces conventions, l'AN2V recommande de s'appuyer sur une approche méthodologique transversale, fondée sur six grandes thématiques complémentaires, regroupées sous l'acronyme SOTAJE :

1. **Stratégie** : définir les objectifs poursuivis et aligner les attentes des élus, des directions et des partenaires.
2. **Organisation** : identifier les acteurs, les ressources humaines mobilisées et les modalités de gouvernance.
3. **Technique** : évaluer les besoins en équipements, logiciels, interopérabilité et connectivité.
4. **Aspects financiers** : structurer un modèle économique soutenable, couvrant investissement et fonctionnement.
5. **Juridique** : assurer la conformité au Code de la sécurité intérieure, au RGPD et aux textes applicables.
6. **Éthique** : garantir le respect des libertés individuelles, la transparence des usages et l'acceptabilité démocratique.



15. SÉCURISER LE PROJET PAR LES CHOIX ADMINISTRATIFS ET CONTRACTUELS

Les choix administratifs et contractuels constituent l'un des angles morts les plus fréquents des projets de vidéoprotection et d'évolution vers des usages de type R2D et à terme, R2A. Ce n'est pourtant ni la caméra ni l'algorithme qui exposent le plus une collectivité, mais bien un marché mal structuré, une dépendance industrielle non anticipée ou des clauses contractuelles déséquilibrées.
Sécuriser le projet suppose donc de traiter ces questions non comme une formalité administrative, mais comme un acte politique engageant la collectivité pour plusieurs années.

15.1. Lorsqu'un projet de vidéoprotection et d'évolution devient un marché public structurant

Un projet de vidéoprotection devient un marché public structurant dès lors qu'il dépasse l'acquisition ponctuelle d'équipements pour engager la collectivité sur plusieurs années, tant sur le plan financier qu'organisationnel. C'est le cas lorsqu'il intègre des infrastructures réseau, des plateformes de supervision, des prestations d'exploitation, de maintenance ou des perspectives d'évolution fonctionnelle au cours du mandat.
Dans ce contexte, le recours à des appels d'offres dits « standards », fondés sur des cahiers des charges techniques très prescriptifs (CCTP) peut dans la plupart du temps correspondre à votre at-

tente, mais peut montrer aussi parfois ses limites en fonction de la complexité du dossier. Le CCTP reflète souvent le niveau de connaissance de celui qui les rédige, qu'il s'agisse d'un service interne ou d'un bureau d'études externe, et tendent à figer prématurément les solutions possibles. Ils peuvent conduire à des réponses conformes mais peu innovantes, voire à des choix techniques difficiles à faire évoluer par la suite.
Pour des projets complexes, évolutifs et fortement structurants, il peut être parfois pertinent de privilégier une approche fondée sur l'expression du besoin fonctionnel plutôt que sur la description détaillée des moyens techniques attendus. Le recours à des procédures comme le marché public global de performance (MPGP) permet alors de laisser aux opérateurs économiques une marge de proposition, tout en encadrant strictement les objectifs, les niveaux de service attendus et les contraintes juridiques.
Cette approche ouvre le champ à des réponses parfois inattendues, mais particulièrement adaptées au territoire. Des acteurs issus du monde des télécommunications, de l'exploitation de réseaux fibre ou de la connectivité peuvent ainsi proposer des solutions intégrées, combinant infrastructures, supervision et services, là où un appel d'offres classique aurait fragmenté les réponses. Cette capacité à agréger des compétences diverses devient un atout majeur dans des projets où la performance repose autant sur le réseau, la disponibilité et la résilience que sur les équipements eux-mêmes.
Ces évolutions interrogent également les modèles techniques traditionnels. Les travaux menés au sein de l'AN2V, notamment dans le cadre du groupe de travail « Hypervision » (GT PUS – plateforme unifiée scalable), illustrent cette tendance à une vision de plus en plus transversale et globale du territoire, intégrant vidéoprotection, capteurs IoT, réseaux et systèmes d'information. De la même manière, les réflexions conduites au sein du groupe de travail « Cloud » montrent l'émergence de modèles de connectivité et d'exploitation virtualisés, susceptibles d'apporter davantage de souplesse, de résilience et de maîtrise dans le temps.
Dans tous les cas, le choix du mode de passation du marché doit rester un acte stratégique. Il ne s'agit pas de rechercher la sophistication pour elle-même, mais de se doter d'un cadre contractuel capable d'accompagner la trajectoire politique définie par la collectivité pour la durée du mandat, sans l'enfermer dans des choix techniques irréversibles ni dépendre d'un modèle industriel unique.

15.2. Les points de vigilance contractuels majeurs

Plusieurs points de vigilance doivent faire l'objet d'une attention particulière lors de la rédaction des marchés publics relatifs à la vidéoprotection et à ses évolutions possibles. Ces points ne relèvent pas de considérations techniques secondaires, mais conditionnent directement la capacité de la collectivité à piloter son dispositif dans la durée, à contenir les coûts et à conserver des marges de manœuvre politiques.
Le premier enjeu concerne la maîtrise des données. Les images, enregistrements, métadonnées et données dérivées doivent rester sous le contrôle effectif de la collectivité, tant sur le plan juridique que technique. Cette exigence conditionne la conformité au RGPD, mais aussi la capacité à faire évoluer l'organisation, à mutualiser ou à changer de prestataire sans rupture de service ni perte d'historique.
La question de la réversibilité est indissociable de cette maîtrise. Un contrat réversible permet à la collectivité de reprendre ses données, de modifier son architecture ou de faire évoluer son dispositif sans dépendre d'un acteur unique. Cette réversibilité doit être explicitement définie, opérationnelle et contractualisée. Elle ne peut se limiter à une déclaration de principe dépourvue de modalités concrètes.
La souveraineté constitue un autre point de vigilance structurant. Elle recouvre à la fois la localisation des données, la maîtrise des infrastructures critiques et la lisibilité des chaînes techniques et contractuelles. Sans tomber dans une approche idéologique, il s'agit pour l'élu d'identifier les risques de dépendance stratégique, voire géopolitique, lorsque des services essentiels reposent sur des acteurs ou des infrastructures situés hors du cadre juridique européen.
La scalabilité du dispositif doit également être anticipée dès la phase de conception du marché. Une solution pertinente à court terme peut devenir rapidement inadaptée si elle ne permet pas une montée en charge progressive, qu'il s'agisse du nombre de caméras, des périmètres couverts, des plages horaires d'exploitation ou des usages. À l'inverse, surdimensionner le dispositif dès l'origine pour des scénarios hypothétiques conduit souvent à des coûts inutiles et à une complexité excessive.
Cette logique de scalabilité ne concerne pas uniquement les logiciels ou les plateformes, mais aussi les infrastructures physiques et réseaux. Anticiper les besoins futurs lors de projets de travaux urbains, d'enfouissement de réseaux, de déploiement de fibre ou de rénovation de l'éclairage public permet de contenir durablement les coûts. La réservation de fourreaux, l'adaptation des supports, la capacité des mâts ou l'accès à l'alimentation électrique constituent des choix structurants, souvent peu visibles politiquement, mais déterminants à moyen terme.
Ces différentes dimensions, maîtrise des données, réversibilité, souveraineté, scalabilité et anticipation des infrastructures, sont étroitement liées. Elles conditionnent la capacité de la collectivité à ajuster son dispositif aux choix politiques du mandat, aux évolutions réglementaires et aux réalités opérationnelles du territoire. Les marchés doivent donc être analysés non seulement à l'aune de leur conformité immédiate, mais aussi de leur aptitude à accompagner une trajectoire sur six ans, sans enfermement technique ni dépendance industrielle excessive.

15.3. Intégrer dès maintenant les contraintes IA Act, CNIL et CSI

Même lorsque certains usages ne sont pas encore autorisés, les cadres réglementaires européens et nationaux s'imposent déjà aux collectivités. L'IA Act européen, les exigences de la CNIL et les finalités définies par le Code de la sécurité intérieure doivent être intégrés dès la conception des marchés.
Cela implique de proscrire toute contractualisation anticipée d'usages non autorisés, même sous couvert d'options ou de clauses conditionnelles mal encadrées. Les marchés doivent au contraire prévoir des mécanismes d'adaptation, permettant d'intégrer de nouveaux usages uniquement lorsque le cadre juridique le permet explicitement.
L'analyse d'impact (AIPD) relative à la protection des données, la documentation des traitements et la traçabilité des accès doivent être pensées comme des obligations structurelles, et non comme des ajustements a posteriori. Cette anticipation est un facteur clé de sécurité juridique pour les élus et les services.

15.4. Clauses types et bonnes pratiques contractuelles

Les clauses contractuelles ne doivent pas être considérées comme un simple formalisme de la procédure, mais comme un outil de pilotage stratégique du projet sur toute la durée du mandat. Bien rédigées, elles protègent la collectivité, sécurisent les élus et préservent la capacité d'évolution du dispositif. Mal conçues, elles enferment durablement la commune dans des choix techniques, financiers ou juridiques difficilement réversibles.
Une première bonne pratique consiste à séparer clairement ce qui est autorisé aujourd'hui de ce qui pourrait l'être demain. Les contrats doivent porter exclusivement sur des usages juridiquement fondés au moment de leur signature. Toute évolution future, notamment en matière de R2A, ne peut être envisagée qu'au travers de mécanismes d'avenants ou de clauses de réexamen explicites, conditionnées à une évolution avérée du cadre juridique et à une décision politique formalisée de la collectivité.
Les clauses relatives à la réversibilité doivent être précises, opérationnelles et vérifiables. Elles doivent définir les modalités concrètes de restitution des données, les formats utilisés, les délais applicables et les responsabilités respectives en cas de changement de prestataire ou d'architecture. Une réversibilité non testée ou non documentée constitue un risque majeur pour la continuité du service public.
La maîtrise des données et de leur hébergement doit également faire l'objet d'engagements contractuels clairs. Les contrats doivent préciser la localisation des données, les conditions d'accès, les sous-traitants éventuels et les obligations en matière de sécurité et de traçabilité. Ces éléments ne relèvent pas uniquement du RGPD, mais de la souveraineté opérationnelle de la collectivité.

Il est également recommandé d'intégrer des clauses garantissant la scalabilité maîtrisée du dispositif. Cela implique de prévoir des mécanismes permettant d'ajuster progressivement les capacités techniques et humaines sans rupture brutale ni surcoût disproportionné. La montée en charge doit être possible, mais jamais imposée par la structure contractuelle elle-même.
Enfin, les bonnes pratiques contractuelles supposent une gouvernance explicite du contrat. Les rôles et responsabilités de la collectivité, du prestataire, du DPO/DPD et des services concernés doivent être clairement définis. Les modalités de suivi, d'audit, de reporting et de contrôle doivent être prévues dès l'origine, afin d'éviter que le contrat ne devienne un objet figé, déconnecté des réalités opérationnelles.
En synthèse, un bon contrat n'est pas celui qui promet tout, mais celui qui laisse à la collectivité la capacité d'arbitrer, d'évoluer et, le cas échéant, de renoncer. C'est cette maîtrise contractuelle qui permet de concilier innovation, conformité juridique et responsabilité politique sur l'ensemble du mandat.

16. GOUVERNER, ÉVALUER ET RENDRE COMPTE SANS ALIMENTER LA DÉFIANCE

La défiance autour de la vidéoprotection ne naît pas principalement des technologies, mais de la manière dont elles sont gouvernées, expliquées et évaluées. Les collectivités qui rencontrent des oppositions durables sont rarement celles qui agissent, mais celles qui donnent le sentiment d'agir sans cadre clair, sans contrôle visible et sans capacité à rendre compte autrement que par des slogans.
Gouverner un dispositif de vidéoprotection, et plus encore ses évolutions possibles, suppose donc une méthode spécifique, fondée sur la clarté politique, la sobriété des indicateurs et une transparence intelligemment organisée.

16.1. Gouvernance politique et rôle structurant du comité d'éthique

La gouvernance d'un dispositif de vidéoprotection ne peut pas être déléguée uniquement aux services techniques ou à la police municipale. Elle relève d'un portage politique explicite, assumé par l'exécutif municipal, et inscrit dans un cadre collectif.
La mise en place d'un comité d'éthique local constitue, à cet égard, un outil structurant. Lorsqu'il est conçu comme un espace de régulation et non comme une instance de communication, il permet de sécuriser les décisions, d'anticiper les risques de dérive et de créer un lieu de débat apaisé, distinct des controverses médiatiques. L'expérience de collectivités pionnières, comme Lyon ou Lille, montre que ce type de comité renforce la solidité politique des projets plutôt qu'il ne les fragilise.
Le comité d'éthique n'a pas vocation à se substituer au conseil municipal ni aux autorités de contrôle, mais à éclairer les choix, à questionner les usages et à documenter les arbitrages. Sa légitimité repose sur sa pluralité, son indépendance relative et la clarté de son périmètre.

16.2. Évaluer sans se noyer dans les indicateurs

L'un des pièges les plus fréquents consiste à vouloir tout mesurer, tout quantifier et tout comparer. Cette inflation d'indicateurs produit rarement de la compréhension et alimente souvent la suspicion.
Une évaluation pertinente repose sur un nombre limité d'indicateurs simples, directement liés aux objectifs affichés par la collectivité. Il peut s'agir de délais de réaction, de taux d'élucidation sur certains types de faits, de continuité de service du CSU ou de capacité à sécuriser des événements spécifiques. Ces indicateurs doivent être stables dans le temps et compréhensibles par des non-spécialistes.
L'enjeu n'est pas de prouver que la vidéoprotection « fonctionne » de manière abstraite, mais de montrer en quoi elle contribue, parmi d'autres leviers, à la sécurité, à la prévention ou à la gestion du territoire.

16.3. Rendre compte régulièrement sans sur-communication

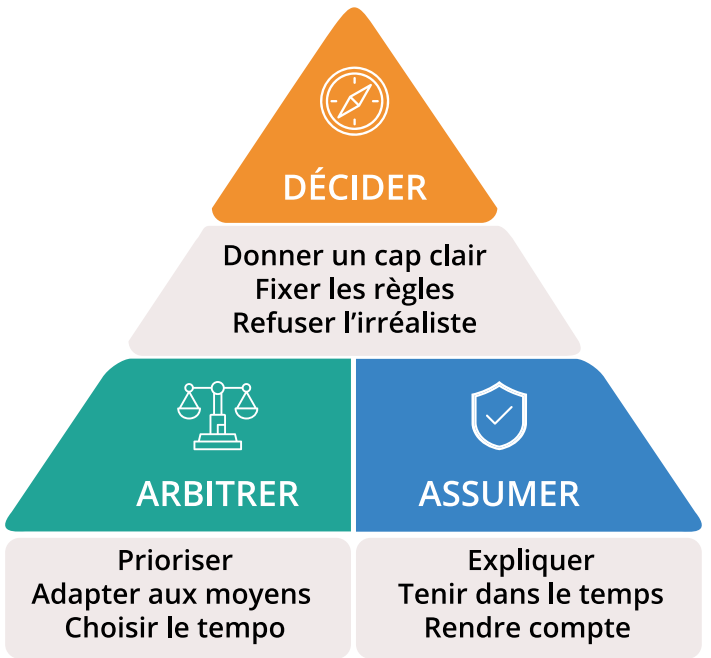
Rendre compte ne signifie pas communiquer en permanence. Une communication excessive, technique ou défensive produit souvent l'effet inverse de celui recherché.
La bonne temporalité est celle du rendez-vous régulier, inscrit dans la vie démocratique locale. Un bilan annuel présenté au conseil municipal, rendu public et contextualisé, suffit dans la plupart des cas. Il doit rappeler les objectifs, présenter les usages réels, signaler les évolutions et assumer les limites du dispositif.
Cette sobriété renforce la crédibilité du discours public. Elle évite de transformer chaque incident, chaque débat ou chaque évolution technologique en polémique, et protège les élus d'une exposition permanente sur des sujets sensibles.

16.4. Gérer les oppositions, les recours et les demandes d'accès

Toute collectivité doit intégrer le fait que des oppositions existeront, indépendamment de la qualité du projet. Chercher à les neutraliser ou à les disqualifier est généralement contre-productif.
La stratégie la plus efficace consiste à distinguer clairement les critiques de bonne foi, les recours juridiques et les postures militantes. Les premières doivent être entendues et traitées dans les cadres existants, notamment via les comités d'éthique ou les instances consultatives. Les secondes relèvent du droit et doivent être instruites avec rigueur, sans dramatisation excessive. Les troisièmes ne doivent pas dicter l'agenda politique de la collectivité.
La transparence procédurale, la documentation des décisions et la traçabilité des usages constituent ici les meilleures protections pour les élus et les services.

16.5. Faire de la transparence un levier de confiance

La transparence n'est pas une exposition totale, mais une capacité à expliquer ce qui est fait, pourquoi cela est fait et dans quelles limites. Elle repose autant sur les mots que sur les actes.
Des initiatives simples, comme l'ouverture ponctuelle d'un CSU lors d'événements publics, la publication de chartes d'usage claires ou la mise à disposition d'informations pédagogiques, contribuent à démystifier les dispositifs sans en révéler les aspects sensibles.
Lorsqu'elle est maîtrisée, la transparence devient un levier de confiance durable. Elle permet de sortir des procès d'intention, de réinscrire la vidéoprotection dans une logique de service public et de rappeler une vérité souvent occultée : la protection des libertés ne s'oppose pas à la sécurité, elle en est une condition.



LEXIQUE

Par ordre alphabétique, quelques acronymes utiles !

ACAP	AXIS Camera Application Platform
AIPD	Analyse d'impact relative à la protection des données
CCTP	Cahier des Clauses Techniques Particulières
CDV	Commission Départementale de Vidéoprotection
CIC/CORG	Centre d'Information et de Commandement/Centre d'opérations et de renseignement de la gendarmerie
CNAPS	Conseil national des activités privées de sécurité
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPP	Centre national de prévention et de protection
CSD	Centre de Supervision Départemental
CSD/CSM	Centre de supervions Départemental / Mutualisé
CSF-IS	Contrat Stratgéique de Filière des Industries de Sécurité
CSI	Code de Sécurité Intérieur
CSU	Centre de Supervision Urbain
CSUi	Centre de Supervision Urbain Intercommunal
DEPSA	Direction des Entreprises et Partenariats de Sécurité et des Armes
DGGN	Direction Générale de la Gendarmerie Nationale
DGPN	Direction Générale de la Police Nationale
DGSCGC	Direction Générale de la Sécurité Civile et de la Gestion des Crises
DLPAJ	Direction des Libertés Publiques et des Affaires Juridiques
DORI	Détection / Observation / Reconnaissance / Identification
DPO	Délégué à la Protection des Données
DPO/DPD	Data Protection Officer... ou Délégué à la Protection des Données
ERP	Établissement Recevant du Public
FFSP	Fédération Française de la Sécurité Privée
FSI	Forces de Sécurité Intérieures
GT	Groupe de Travail
GTI/GTR	garantie de temps d'intervention /rétablissement
IA	Intelligence Artificielle
IA Act	Loi sur l'IA de l'UE : première réglementation de l'IA...
IHM	Interface Homme-Machine
LAPI/LPI/VPI	Lecture automatisée de plaques d'immatriculation / Lecture de plaques d'immatriculation / Visualisation de plaque d'immatriculation
MCI	Main courante informatique
OCR	Optical Character Recognition
ONVIF	"Open Network Video Interface Forum" est un forum mondial ouvert, créé en 2008
OPJ	Officier de Police Judiciaire
PN/GN	Police Nationale / Gendarmerie Nationale
POC	Proof of Concept
PP / PPP	Préfectude de Police / de Paris
PPMS	Plan Particulier de Mise en Sûreté
PTI	Protection Travailleur Isolé
PTZ	Pan Tilt Zoom
QoS	Quality of Services
R2A	Remontée Automatique d'Alerte
R2D	Remontée Automatique de Données
RACI	Matrice Responsabilité / Approbation / Consultation / Information
RGPD	Règlement Général sur la Protection des Données
SGDSN	Secrétariat général de la Défense et de la Sécurité nationale
SIG	système d'information géographique
SNR	Stratégie nationale de résilience
SOTAJE	Strat / Orga / Technique / Aspect financier / Juridique / Ethique
TMS	troubles musculo–squelettiques
VAMA	Vol à Main Armée
VSA	Video Surveillance Augmentée
VSAAS	Video Surveillance as a Service
WDR	Wide Dynamic Range - Plage dynamique étendue

AN2V

ANTICIPER,
DÉFENDRE,
PARTAGER !

an2v.org

L'AN2V, le cercle de réflexion technico-juridique
qui réunit tous les acteurs de la sécurité/sûreté :

25 ÉVÉNEMENTS ORGANISÉS PAR AN
8 500 MEMBRES ACTIFS
9 GROUPES DE TRAVAIL
7 000 GUIDES PIXEL DISTRIBUÉS
20 CONFÉRENCES PAR AN
50 INTERVIEWS PAR AN

PIXEL
BIBLIOTHÈQUE MEMBRES
INNOVATION DU VENDREDI
RÉUNION THÉMATIQUE
GROUPE DE TRAVAIL

ÉVÈNEMENT AN2V
CLUB AN2V
SALON PROFESSIONNEL
FORMATION AN2V

Participer à l'AN2V,
c'est gagner du temps, élargir son réseau
et construire la sécurité de demain, ensemble !

VIDÉOPROTECTION

Le livre blanc au service les ÉLUS et les FUTURS ÉLUS

Les collectivités font face à des attentes fortes : **sécurité du quotidien, tranquillité publique, gestion des incivilités, optimisation des moyens**. La vidéoprotection et l'automatisation ne sont pas des solutions "magiques", mais **des leviers concrets** quand elles sont pensées avec **méthode, cadre légal et objectifs clairs.**



Ce livre blanc vous aide à :

- Comprendre vite ce que la vidéoprotection et l'IA peut (et ne peut pas) faire.
- Décider sereinement : priorités, choix techniques, coûts, gouvernance.
- Déployer correctement : cadre réglementaire, éthique, cybersécurité, marché public.
- Obtenir des résultats mesurables : usage au service des équipes et des habitants.

Vous y trouverez :

- Les **points clés** pour lancer ou remettre à niveau un projet.
- Les **erreurs fréquentes** à éviter.
- Des repères de **bonnes pratiques** terrain.
- Des **check-lists** simples pour passer à l'action immédiatement.

Pour concilier sécurité, efficacité et libertés publiques.

AN2V