Sujet élaboré par une cellule pédagogique nationale

CONCOURS EXTERNE, INTERNE ET TROISIÈME CONCOURS DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2e CLASSE

SESSION 2026

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 27 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 2e classe au sein de la direction des systèmes d'information en tant que chef de projet informatique, dans la collectivité de Techniville (45 000 habitants), ville centre d'un EPCI.

Techniville possède un système de vidéoprotection obsolète maintenu avec difficulté, et qui doit impérativement faire l'objet d'un renouvellement.

Dans un premier temps, le directeur des systèmes d'information vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur la vidéoprotection.

10 points

Les élus souhaitent mener une réflexion sur la modernisation du système, de manière mutualisée et sécurisée, à l'échelle de l'EPCI.

Dans un deuxième temps, le directeur des systèmes d'information vous demande d'établir un ensemble de propositions opérationnelles visant à mettre en œuvre cette évolution de la vidéoprotection, à l'échelle de l'EPCI.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances.

10 points

Liste des documents :

Document 1 : « Les 5 lauréats de l'appel à projets "Territoires intelligents durables" enfin dévoilés » - (extrait) - *lagazette.fr* - 26 octobre 2022 - 2 pages

Document 2 : « Vidéoprotection : comment permettre aux communes de conserver un matériel de dernière génération ? » - *lagazette.fr* - 24 janvier 2024 - 1 page

Document 3 : « Comprendre l'évolution du droit de la vidéoprotection » (extrait) - *lagazette.fr* - 22 juillet 2025 - 3 pages

Document 4 : « Renforcer la sécurité et la sûreté » (extrait) - *eiffageenergiesystemes.com* - 20 octobre 2025 - 2 pages

Document 5 : « Vidéoprotection et Système d'information sécurisé, deux notions indissociables ! » - Patrice Duhem - *on-x.com* - 26 novembre 2024 - 1 page

Document 6 : « Une bonne caméra de vidéoprotection coûte entre 7.500 et 12.500 euros à une commune » (extrait) - *francebleu.fr* - 24 mars 2025 - 2 pages

Document 7 : « Les dépôts sauvages dans le viseur des caméras intelligentes » (extrait) - *lagazette.fr* - 16 septembre 2024 - 3 pages

Document 8 : « Kit caméra de surveillance pour collectivités : guide complet pour choisir et déployer votre système (extrait) » - *leaseprotect.fr* - 9 décembre 2024 - 4 pages

Document 9 : « Vidéosurveillance intelligente : les usages controversés du logiciel Briefcam » - *lagazette.fr* - 8 janvier 2024 - 2 pages

Document 10 : « Sécurisation d'un réseau informatique dédié à la vidéoprotection. Systèmes et contrôle» (extrait) - Julien Trelat - *dumas.ccsd.cnrs.fr* - 29 novembre 2021 - 2 pages

Document 11 : « L'installation d'un système de vidéosurveillance » (extrait) - *telesurveillance-videosurveillance.fr* - 17 décembre 2025 - 2 pages

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

Dans un souci environnemental, les impressions en noir et blanc sont privilégiées. Les détails non perceptibles du fait de ce choix reprographique ne sont pas nécessaires à la compréhension du sujet, et n'empêchent pas son traitement.

DOCUMENT 1

Adresse de l'article https://www.lagazettedescommunes.com/833001/les-5-laureats-de-lappel-a-projets-territoires-intelligents-durables-enfin-devoiles/ (extrait)

AMÉNAGEMENT NUMÉRIQUE

Les 5 lauréats de l'appel à projets « Territoires intelligents durables » enfin dévoilés

Laura Fernandez Rodriguez | France | Publié le 26/10/2022

Trois syndicats, une région, une métropole : les lauréats de la première vague de l'appel à projets «Territoires intelligents et durables » de France 2030 sont enfin connus. L'Avicca se réjouit pour les collectivités retenues, mais appelle à sortir d'une logique d'appel à projets au profit d'un véritable guichet de long terme.

Le suspense est enfin levé. Mardi 25 octobre, ont officiellement été dévoilés les 5 premiers lauréats de l'appel à projets «Territoires intelligents et durables ». Une annonce attendue qui avait été reportée à plusieurs reprises.

Le syndicat départemental d'électrification du Finistère (Bretagne), le syndicat intercommunal d'énergie de l'Ain (Auvergne Rhône Alpes), Toulouse métropole (Occitanie), la région Grand Est, et le syndicat audois de l'énergie et du numérique (Occitanie) sont les 5 lauréats, sur les 16 candidatures qui avaient été déposées pour cette première vague.

Des territoires en capacité de mutualiser

Voici le détail des projets retenus, qui sont plutôt macros et comportent souvent une dimension « safe cities » avec la mention de la vidéoprotection :

- Pour le syndicat départemental d'électrification du Finistère, le déploiement à grande échelle d'une infrastructure Lora, le déploiement de services d'objets connectés dans une logique de transition énergétique (éclairage public, efficacité énergétique des bâtiments, collecte de déchets, qualité de l'air intérieur), avec un objectif de mutualisation et cofinancement pour rendre ces services accessibles aux plus petites collectivités ;
- Pour le syndicat intercommunal d'énergie de l'Ain, un projet centré sur le « déploiement d'un hyperviseur permettant de centraliser la gestion des réseaux et équipements » dans une logique prédictive (éclairage

public, fibre optique, énergétique photovoltaïque, vidéoprotection, etc) ;

- Pour Toulouse métropole, un projet basé sur l'exploitation d'une plateforme permettant de créer de la valeur sur l'exploitation de données territoriales (efficacité énergétique, opérationnelle dans l'expoitation des ouvrages, conformité, planification et suivi de travaux, etc), tout en pensant la réplicabilité du modèle ;
- Pour Grand Est, le déploiement de solutions d'hypervision dans des collectivités rurales associant un réseau d'interconnexion passive d'équipements, en lien avec la ville intelligente (signalisation, vidéoprotection, stationnement, eau, déchets, etc), avec la volonté de permettre un passage à l'échelle ;
- Pour le syndicat Audois de l'énergie et du numérique, « la structuration d'un système organisé et interopérable de management des territoires intelligents à l'échelle départementale avec la constitution d'une infrastructure numérique souveraine (GFU) et d'un panel de services mutualisés adaptés aux petites communes », le développement d'un écosystème pour la résilience face aux changements climatiques (prévention des feux de forêt et des inondations), ainsi qu'un soutien au développement économique du territoire par l'appui à l'innovation technologique.

A l'Avicca, on se réjouit pour les projets lauréats, dont 4 sont portés par des membres de l'association : « Nous sommes satisfaits qu'il y ait 4 territoires et une métropole, car les territoires intelligents et durables, ce ne sont pas que des projets pour les villes, ce sont des projets de territoires, et en l'occurrence ici des territoires qui soient en capacité de mutualiser les efforts faits sur ces sujets, comme des syndicats et même la région Grand Est », relève Luc Derriano, chargé de mission à l'Avicca.

Tension ou convergence ?

Y a-t-il une tension entre les termes « intelligent » et « durable », un sujet qui peut paraître confusant aux yeux de certaines collectivités chargées de s'engager par exemple dans la transformation numérique tout autant que dans le numérique responsable, notamment à la suite de la loi REEN ?

« Nous sommes interpellés par certains adhérents sur ce sujet, nous y travaillons en interne pour que des élus du CA puissent le porter politiquement et techniquement. Mais nous pensons que cette « tension » peut tout à fait se résoudre dans la pratique. Par exemple, le déploiement de capteurs peut se faire au service de moindres dépenses énergétiques, d'une meilleure qualité de l'air, de mobilités alternatives et intelligentes, etc… Il est possible d'ajouter de nouveaux services ou capteurs tout en se préoccupant de ne pas alourdir le bilan carbone de la collectivité », estime Luc Derriano.

AAP vs guichet de long terme

A noter enfin qu'une deuxième vague, complétée par un volet IA, « frugale et au service des objets de décarbonation et de transition énergétique des territoires », a été ouverte, jusqu'au 7 novembre prochain à 17h.

L'Avicca considère toutefois que les AAP ne peuvent pas constituer une politique publique pérenne et durable sur ces sujets, et plaide pour un plan « France territoires durables et connectés », structuré avec un guichet ouvert sur plusieurs années, à la manière de ce qui a été fait pour le plan France très haut débit.

« Au lieu de mettre les collectivités dans une situation où elles doivent répondre rapidement, sur des projets structurants et complexes à concevoir puis mettre en œuvre sur de multiples niveaux, de gouvernances, juridiques, financiers, nous plaidons pour une adaptation au rythme des collectivités », détaille-t-il. Le risque étant sinon que, selon la formule du président de l'Avicca et sénateur de l'Ain, Patrick Chaize, « l'AAP arrose souvent là où il pleut déjà ».(...)

Adresse de l'article https://www.lagazettedescommunes.com/909359/videoprotection-comment-permettre-aux-communes-de-conserver-un-materiel-de-derniere-generation/

SÉCURITÉ

Vidéoprotection : comment permettre aux communes de conserver un matériel de dernière génération ?

Léna Jabre | Réponses ministérielles | Réponses ministérielles finances | Réponses ministérielles prévention-sécurité | Publié le 23/01/2024 | Mis à jour le 24/01/2024

Réponse du ministère de l'Intérieur et de l'outre-mer : Outre les crédits disponibles dans le cadre du Fonds interministériel de prévention de la délinquance (FIPD, 82 M€ en 2023), les dotations de soutien à l'investissement des collectivités territoriales (DETR, DPV, DSIL, DSID) soutiennent déjà de nombreux projets d'investissement dans le domaine de la vidéoprotection : en 2022, 648 projets ont été soutenus par l'Etat, qui a attribué 18,2 M€ de subvention (dont 3,5 M€ au titre de la DETR, 13,9 M€ au titre de la DSIL, 0,2 M€ au titre de la DPV, et 0,6 M€ au titre de la DSID).

Entre 2018 et 2022, 2236 projets ont été cofinancés par l'Etat dans ce domaine, soit un montant total subventionné de 69,1 M€. 1742 collectivités ont été accompagnées dans 93 départements. La dépense d'investissements correspondante s'élève à 180,3 M€, soit un effet de levier de 2,6.

L'Etat soutient donc activement les collectivités qui présentent ce type de projets.

En plus des projets classiques d'équipements, plusieurs projets de création et d'aménagement de centres de supervision urbains ont d'ailleurs été sélectionnés par les préfets ces dernières années, par exemple ceux portés par les communes de Choisy-le-Roi (94), Champigny-sur-Marne (94), Ouistreham (14) et Toul (54). En ce qui concerne les dépenses de fonctionnement liées à ces matériels (entretiens, location, etc.), le soutien de l'Etat passe par la dotation globale de fonctionnement (DGF), dont le montant a été accru en 2023 pour la première fois depuis 10 ans, à hauteur de 320 M€.

REFERENCES

- Question écrite d'Emmanuel Blairy, n°6234, JO de l'Assemblée nationale du 26 décembre.

DOSSIER : L'innovation publique à l'épreuve du droit
Dossier publié à l'adresse https://www.lagazettedescommunes.com/910304/comprendre-levolution-du-droit-de-la-videoprotection/ (extrait)

FICHE PRATIQUE

Comprendre l'évolution du droit de la vidéoprotection

Auteur associé | Actu juridique | Fiches de droit pratique | France | Publié le 31/01/2024 | Mis à jour le 22/07/2025

Le cadre juridique de la vidéoprotection est mouvant. Dernière modification en date : la loi du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024. Décryptage des différentes évolutions juridiques en la matière.

Bien distinguer les types de caméras et d'utilisations

L'usage de caméras sur la voie publique peut relever de deux grandes finalités distinctes : la vidéoverbalisation et la vidéoprotection. La verbalisation automatique par caméra n'est, en principe, pas admise (cf. loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, art. 95). En revanche, les fonctionnaires de police peuvent, pour certaines infractions au code de la route (listées à l'article R.121-6), dresser le procès-verbal d'infraction en « capturant » des images issues des caméras sur voie publique. Ce régime connaît un encadrement propre et appelle notamment une information des usagers.

Proche mais distinct, le dispositif de lecture automatisée des plaques d'immatriculation (Lapi) permet de contrôler et de sanctionner le paiement de la redevance de stationnement sur la voie publique. Mais il ne s'agit pas là de verbaliser, puisque ledit stationnement ne relève plus, depuis le 1er janvier 2018, de la police et des amendes, mais d'une redevance « forfaitaire post-stationnement », dont le montant est librement fixé par les collectivités. Les caméras utilisées sont le plus souvent mobiles et ne se confondent généralement pas avec celles utilisées pour la videoprotection ou la verbalisation.

Il ne saurait en aller autrement, selon la Commission nationale de l'informatique et des libertés (Cnil). Celle-ci a rappelé dans un avis du 25 août 2020 que, « en l'état actuel de la réglementation, il est interdit pour les communes de recourir à des dispositifs de verbalisation automatisée reposant sur la photographie du véhicule et de sa plaque d'immatriculation pour la recherche et la constatation d'infractions ». Le message est clair et rappelé à maintes reprises : la vidéoverbalisation, par exemple du stationnement gênant, est interdite.

Comprendre pourquoi il fallait changer le droit de la vidéoprotection

La matière a connu d'importants changements, qui ne sont pas toujours bien mesurés. Le seul cadre législatif régissant les systèmes de vidéoprotection a longtemps été constitué par un dispositif reposant, d'une part, sur la loi n°95-73 du 21 janvier 1995, dite « Lopsi 1 », codifiée par la suite au code de la sécurité intérieure (CSI), d'autre part, sur la loi « informatique et libertés » n°78-17 du 6 janvier 1978.

Dans ce cadre, les systèmes de vidéoprotection étaient définis par l'article L.251-1 du CSI comme des « enregistrements visuels », soumis aux dispositions du CSI ou, lorsqu'ils permettaient, par un traitement automatisé, d'identifier, directement ou indirectement, des personnes physiques, aux dispositions de la loi « informatique et libertés ». Complément important à cette répartition, un avis du Conseil d'Etat (CE, 24 mai 2011, avis n° 385125) de mai 2011 avait posé que les systèmes de vidéoprotection « traditionnels » n'étaient pas pourvus, en principe, des fonctionnalités permettant d'identifier les personnes physiques. Par voie de conséquence, la majorité des dispositifs de vidéoprotection n'étaient régis que par le régime issu du CSI.

En 2016, le règlement général sur la protection des données (RGPD) n° 2016/679 et la directive (UE) « police-justice » n°2016/680 du 27 avril 2016 ont entièrement bouleversé le régime applicable à la vidéoprotection. En instaurant un cadre européen de traitement des données à caractère personnel, ces textes sont également venus régir le traitement de données « à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales », en conférant à la notion de « traitement » une acception particulièrement large (collecte, enregistrement, consultation, utilisation…).

En d'autres termes, à partir de 2016, non seulement les enregistrements visuels constitutifs de la vidéoprotection doivent être appréhendés comme des traitements de données régis par le droit européen, mais la simple consultation des images captées par des caméras de vidéoprotection caractérise également un traitement de données au sens européen.

Cette révolution silencieuse, non intégrée par le droit français pendant des années, était lourde de conséquences. Grâce à ce « paquet européen » de protection des données personnelles, les personnes concernées par le traitement de leurs données voient renforcer et étendre (notamment à la vidéoprotection) les droits dont ils disposent.

Notamment leurs droits d'accès, de rectification, de modification, d'effacement, de limitation et d'opposition au traitement de leurs données. La transposition du RGPD et de la directive « police-justice » au sein des titres II et III de la loi « informatique et libertés » ont bien eu lieu. Mais, jusqu'à 2023, cette évolution majeure a été ignorée par le CSI, dont les dispositions étaient pourtant obsolètes.

Identifier ce que la loi relative aux JO du 19 mai 2023 a définitivement changé

La loi n° 2023-380 du 19 mai 2023 relative entre autres aux Jeux olympiques et paralympiques de 2024 n'a pas eu une simple portée conjoncturelle : à cette occasion, le législateur a modifié les dispositions du CSI portant sur la vidéoprotection, pour les mettre en conformité avec le droit issu de l'Union européenne.
L'article L.251-1 dudit code ne vise plus seulement les enregistrements visuels mais, plus largement, « les systèmes de vidéoprotection », lesquels « sont des traitements de données à caractère personnel régis par le présent titre, par le [RGPD] et par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » ayant transposé, en son titre III, la directive « police-justice ».

Exit, donc, la vidéoprotection uniquement caractérisée par les enregistrements visuels, à l'instar de l'application alternative des régimes issus du CSI et de la loi « informatique et libertés ». La définition de la vidéoprotection ainsi que le régime – théoriquement – applicable semblent désormais cohérents avec le cadre normatif européen. Ce sera, là aussi, un « héritage » inattendu et bienvenu des JO.

S'agissant de la mise en œuvre des systèmes de vidéoprotection, il faut être clair : le nouveau régime se traduit par un alourdissement de la procédure. En complément de l'autorisation préfectorale requise (CSI, art. L.252-1), la vidéoprotection qui recourt à un traitement, par les « autorités compétentes », de données personnelles

intéressant la sécurité publique ou ayant pour objet la recherche, la constatation et la poursuite d'infractions pénales doit également faire l'objet d'une autorisation du ministre compétent, après avis motivé de la Cnil

(loi « informatique et libertés », art. 31).

Mesurer l'incohérence du régime actuel de la vidéoprotection

L'application de ce nouveau régime se heurte toutefois à une difficulté pratique et juridique notable. Le « paquet européen » a certes renforcé les droits des personnes concernées par le traitement de leurs données personnelles. Mais il ne nous a pas donné le mode d'emploi permettant de rendre effectif l'exercice de ces droits. En particulier, il est évidemment malcommode, voire impossible, pour les personnes filmées sur la voie publique de s'opposer concrètement au traitement de leur image, ou même de le rectifier.

Ce sujet est identifié depuis longtemps. Au point que la Cnil avait alerté le législateur par la délibération 2022-118 du 8 décembre 2022. Elle relevait alors que « les modifications apportées par la loi ne permettront pas de résoudre les difficultés plus spécifiques d'articulation entre le CSI et la réglementation en matière de protection des données à caractère personnel ». Elle préconisait que le CSI soit complété, le cas échéant par le pouvoir réglementaire, afin d'apporter trois modifications indispensables : écarter explicitement le droit d'opposition ; prévoir une information des personnes concernées ; clarifier la question du droit d'accès aux enregistrements.

La mise en garde de la Cnil a été entendue et le nouvel article L.255-1 du CSI issu de la loi « JO » du 19 mai 2023 prévoit qu'un décret en Conseil d'Etat, pris après avis de la Cnil, fixera les conditions dans lesquelles les personnes concernées peuvent exercer leurs droits. On peut donc raisonnablement prévoir que le droit d'opposition sera bientôt explicitement exclu dans le cadre spécifique de la vidéoprotection.

Dans l'attente de la parution de ce décret, et dans un souci de cohérence effective avec le droit européen, il

convient certainement de se référer aux articles 107 et 110 de la loi « informatique et libertés », desquels l'on peut déduire que c'est à l'acte instaurant le système de vidéoprotection – l'arrêté préfectoral éventuellement complété de l'arrêté ministériel pris après avis de la Cnil – de restreindre les droits des personnes.

Utiliser l'intelligence artificielle (IA) ou la craindre ?

Les enjeux sont renouvelés par la possibilité (et la pratique) de traiter les images de vidéoprotection en utilisant l'intelligence artificielle : détection automatique de comportements, de présence d'objets (tels des déchets) ou d'animaux, comptage de fréquentation… Cette évolution n'était pas prévue par les textes, qui étaient muets à son sujet. A la question de savoir comment appréhender cette nouveauté, la Cnil répond avec fermeté qu'il s'agit d'un véritable bouleversement, un changement tel que l'interdiction lui semble devoir prévaloir, l'autorisation restant l'exception.

L'article 10 de la loi « JO » du 19 mai 2023 s'inscrit dans cette logique en n'autorisant qu'à titre expérimental, et jusqu'au 31 mars 2025, la mise en œuvre de traitement algorithmique d'images résultant des systèmes de vidéoprotection. Seuls certains évènements spécifiques autorisent l'utilisation des caméras intelligentes, et seulement pour détecter des évènements précisément identifiés. Pour autant, certaines voix s'élèvent pour défendre que l'IA, hors l'hypothèse de détournement frauduleux, est peut-être plus respectueuse des données personnelles que les systèmes existants. Le sujet appelle sa propre étude.

(...)

DOCUMENT 4

« Renforcer la sécurité et la sûreté » (extrait)

eiffageenergiesystemes.com - consulté le 20/10/2025

La sécurité et la sûreté sont aujourd'hui au cœur des préoccupations des Français. Selon un sondage Elabe, elles arrivent en seconde position, juste après les enjeux de santé. Conscientes de ces fortes attentes, les villes se réinventent pour offrir un cadre sécurisant et agréable à leurs habitants. Qu'il s'agisse de sécurité dans les rues, sur les routes ou encore de prévenir les risques naturels, les villes ont besoin des nouvelles technologies pour protéger leurs habitants.

Eiffage Énergie Systèmes vous accompagne pour mettre en place ces dispositifs innovants. Caméras haute définition (HD) pour la vidéo surveillance, capteurs intelligents, éclairage public avec détecteur de mouvements …, nous vous offrons un large panel de solutions.

(...)

La vidéo protection pour détecter les incidents

Afin de lutter contre les incivilités, de plus en plus de communes mettent en place un système de **vidéo protection**. Des caméras sont alors installées dans des lieux stratégiques et l'ensemble est relié à un centre de protection urbaine qui permet leur exploitation. Cette surveillance repose sur la prévention, la dissuasion et l'assistance des forces de sécurité.

Eiffage Énergie Systèmes a notamment déployé de nouvelles caméras HD dans la commune de Crépy-en-Valois (Oise). Ce système permet un maillage vidéo précis du territoire afin d'améliorer la sécurité des personnes et la protection des biens. Toutes les images sont transférées vers le poste de police municipale. Elles sont stockées pour être analysées en cas d'infractions.

"Il s'agissait d'optimiser notre système de vidéo protection pour améliorer la sécurité des personnes et la protection des biens. »

Gilles Bouttier – Responsable police municipale de Crépy-en-Valois

Optimiser les infrastructures existantes

Les capteurs intelligents renforcent également la sécurité d'une ville. Ils peuvent, par exemple, être installés sur les infrastructures de l'éclairage public pour gérer son intensité lumineuse en fonction du mouvement. En cas de passage, la lumière devient plus forte et offre un ressenti sécurisant pour l'usager. Eiffage Énergie Systèmes a notamment mis au point une solution baptisée Luciole® pour réguler l'éclairage public. L'intensité lumineuse varie en cas de présence de 20% à 100% de sa capacité pour un éclairage optimum.

Nos solutions permettent ainsi une anticipation du risque pour mettre en œuvre les moyens nécessaires. Elles permettent ainsi le monitoring du niveau d'un cours d'eau en amont d'une installation à protéger ou encore la protection des sous-sols de bâtiments potentiellement inondables.

Superviser et piloter les ressources disponibles avec l'hyperviseur

Avec les objets connectés, de nouvelles perspectives de pilotage des infrastructures publiques, s'ouvrent pour les collectivités : adapter au juste besoin les tournées de prélèvement des déchets, la maintenance du matériel d'éclairage, le suivi des infractions routières…Il est alors possible pour les décideurs de réunir toutes les informations sur une même plateforme qui permettra toute une nouvelle dynamique d'administration.

L'hyperviseur Expercité est une véritable solution de pilotage ouverte et non propriétaire et permet de fédérer les différents métiers de la collectivité pour les rendre plus efficients. Les domaines d'applications sont illimités, mais définis, à chaque fois, en fonction des besoins des utilisateurs et des problématiques à traiter.

Une offre clés en mains

En fonction de sa taille et de son urbanisation, chaque ville répond à des problématiques différentes. Les choix techniques utilisés sont donc variables : système ultra HD, caméra dôme 360°, lecture tout temps de plaques d'immatriculations… Les équipes Eiffage Énergie Systèmes proposent des offres clé en main, de l'étude à la maintenance en passant par la réalisation des travaux.

Nous avons, par exemple, répondu aux contraintes de la ville d'Albi (Tarn). Cette municipalité avait besoin d'adopter des caméras ultra HD pour exploiter les images en différé qui lui permettent de gérer sa sécurité. Grâce à ce dispositif, il est désormais possible d'effectuer un zoom dans l'image déjà enregistrée sans altérer sa netteté.

(...)

DOCUMENT 5

« Vidéoprotection et Système d'information sécurisé, deux notions indissociables ! »

Patrice Duhem - on-x.com - 26/11/2024

La vidéoprotection se déploie de façon exponentielle dans tous les secteurs de la vie économique et de l'administration, avec pour obsession légitime la protection des personnes et des biens. Les collectivités, comme les sociétés privées, consacrent des budgets importants chaque année à l'installation de caméras, de plus en plus « intelligentes ».

Aussi surprenant que cela paraisse, il s'avère que Vidéoprotection et Cybersécurité vivent dans des mondes parallèles dans la majorité des organisations. Pourtant les systèmes de vidéoprotection d'une part, traitent, stockent et échangent des données personnelles, et d'autre part sont installés sur un ou plusieurs réseaux informatiques susceptibles d'être la cible d'attaquants, ce qui devrait inciter ces deux pôles à travailler main dans la main.

Aujourd'hui, dans la plupart des organisations, la Vidéoprotection (étude, mise en place, fonctionnement) est confiée au Responsable Sûreté et Sécurité ou au Responsable des Services Généraux, qui a la compétence Sûreté périmétrique, mais pas toujours la compétence Cybersécurité, et sur ce point il fait souvent confiance à ses fournisseurs, à tort ou à raison.

De son côté, le Responsable des Systèmes d'Information (RSI) n'est en général pas sollicité, alors que la sécurisation des SI supportant le fonctionnement de la Vidéoprotection est pourtant indispensable dans un contexte où la menace de cyberattaque est très élevée, la règlementation de plus en plus prégnante et l'hybridation de la criminalité de plus en plus forte (attaques physiques et numériques combinées).

Globalement, les systèmes d'information supportant la Vidéoprotection sont très peu ou mal sécurisés, alors qu'ils traitent des flux de données de plus en plus volumineux, et qu'ils sont souvent interconnectés au SI général de l'entité. De plus, l'utilisation de dispositifs sophistiqués comme les caméras dites « intelligentes » expose ces SI aux cybermenaces autant qu'elle est bénéfique à la surveillance des espaces.

Le risque pour ces SI est principalement de trois ordres :

- **Le vol de données, par un attaquant, ayant exploité une vulnérabilité sur le SI de vidéoprotection.** Les données récupérées sont ainsi revendues sur le darknet. Le manque de sécurisation des données vidéos a un impact significatif sur la conformité de l'organisation au RGPD. Un vol avéré pourrait mener à un contrôle et une sanction de la CNIL.
- **La prise de contrôle du système de vidéoprotection**. Dans ce contexte un attaquant peut naviguer sur le réseau de Vidéoprotection afin d'intervenir sur son fonctionnement et sur le paramétrage des dispositifs de sécurité (caméras, enregistreur, serveur VMS). Une compromission du réseau de vidéoprotection peut aussi avoir pour but de chercher une entrée sur le SI général de l'entité, le compromettre et attenter à l'activité de l'organisation.
- **Le blocage du système de vidéoprotection** qui se matérialise par l'inopérabilité des dispositifs peut aussi être l'occasion d'une demande de rançon (ransomware) en contrepartie d'une remise en état très hypothétique du système.

Pour limiter ces risques, l'organisation doit considérer son système de vidéoprotection comme un SI à part entière et le sécuriser à l'image des autres SI gérés par le Responsable des Systèmes d'Information.

L'intégration de la cybersécurité dans les nouveaux projets d'installation, ou d'extension de systèmes de vidéoprotection, comme l'évaluation de la cybersécurité des sites déjà installés, permettent de réduire efficacement les risques décrits précédemment. Ces analyses permettent une consolidation d'un plan d'actions de sécurisation de ces systèmes de vidéoprotection.

Il est important de rappeler que le besoin de cybersécurité doit s'analyser autant sur le plan opérationnel que règlementaire.

DOCUMENT 6

« Une bonne caméra de vidéoprotection coûte entre 7.500 et 12.500 euros à une commune » (extrait)

Francebleu.fr - 24/03/2025

L'adjudant Éric Wilfart, membre de la cellule de prévention technique de la malveillance (CPTM) © Radio France - © Quentin Perez de Tudela

Dans les zones périurbaines et rurales, de plus en plus de communes du Gard adoptent cet outil pour lutter contre l'insécurité. Pour les installer, elles peuvent être accompagnées par les gendarmes du Gard. Décryptage.

Depuis longtemps déjà, la vidéoprotection a séduit les grandes villes du Gard. Parmi elles : **Nîmes, 2e ville de France** avec le plus grand nombre de caméras par habitant après Nice.

Dans les campagnes du département cela-dit, de plus en plus de communes adoptent cet outil, pour **repousser, dissuader ou identifier d'éventuels délinquants**. Ici Gard Lozère a donc décidé de faire le point.

En zones périurbaines et rurales, combien de communes sont équipées dans le Gard ?

Si on part du principe que ces territoires correspondent, à peu près, aux communes en zone gendarmerie (il y en a 343 en tout), on arrive à **135 communes équipées dans le département**. Toutefois, ce chiffre est sans doute en-deçà de la réalité, dans la mesure où il ne prend en compte que les mairies qui ont dit aux forces de l'ordre qu'elles avaient installé des caméras ; une démarche qu'elles ne sont pas obligées d'effectuer.

Les gendarmes peuvent accompagner les élus qui souhaitent en installer

Au sein du groupement de gendarmerie du Gard, il y a un service spécialisé. Son nom : la CPTM, la cellule de prévention technique de la malveillance. Elle est composée de deux agents, chargés notamment de conseiller les élus pour trouver les endroits les plus pertinents où installer ces caméras. L'adjudant Éric Wilfart en fait partie : *"Une commune va chercher à protéger ses propres biens, ses installations, ses écoles et autres édifices publics*, souligne le militaire. *Nous, les gendarmes, allons plutôt chercher à vouloir, dans le cadre d'une enquête, identifier les personnes qui entrent ou qui sortent d'une commune. Résultat :* ***le lieu où peut être installée une caméra fait l'objet d'une discussion*** *entre les deux parties."* À la fin, cependant, c'est la commune qui tranche, dans la mesure où elle tient les cordons de la bourse.

Quelle efficacité ?

Le recours à ces caméras fait régulièrement l'objet de débat. **Débat éthique, débat philosophique**. Au-delà des discours théoriques, il y a la pratique. Voici un cas très concret dans lequel la vidéoprotection a fait la preuve de son efficacité, dans le Gard : *"L'*agression d'une joggeuse à Vergèze, rappelle l'adjudant Éric Wilfart. *Avec la description du suspect faite par les témoins et le recoupement effectué avec les images vidéo, le mis en cause a pu être rapidement identifié"*, souligne l'intéressé qui s'empresse d'ajouter : *"Les caméras sont un outil pour mener une enquête, mais il ne faut pas tout miser dessus."*

L'exploitation des images de vidéoprotection reste très encadrée

Les caméras ne doivent filmer **que les espaces et les bâtiments publics**. Les maisons et les jardins privés, par exemple, doivent être floutés. Ce floutage peut être levé, mais uniquement à la demande des enquêteurs et sur décision d'un juge, dans le cadre d'affaires particulièrement graves.

Par ailleurs, les mairies sont obligées de demander à la préfecture l'autorisation d'installer des caméras. Elles ont un document à remplir, un CERFA. Si un élu oublie de le faire, il s'expose à **une peine qui peut aller jusqu'à cinq ans de prison et 300.000 euros d'amende**.

Le prix de la caméra, lui, est plutôt salé

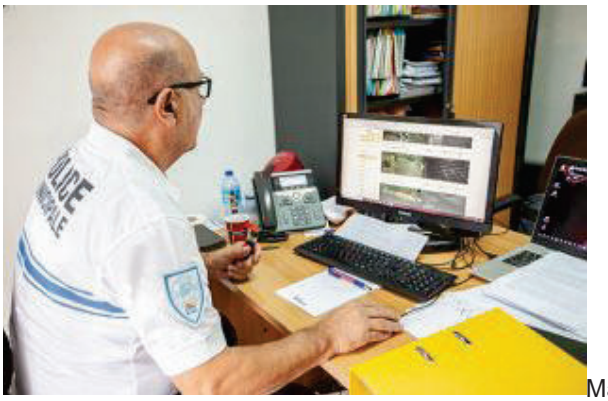
Selon l'adjudant Éric Wilfart, une bonne caméra coûte **plusieurs milliers d'euros**. *"Oui, entre 7.500 et 12.500 euros*, dit-il. *Cette fourchette de prix*, poursuit le militaire, *inclut notamment : les licences informatiques, le rapatriement des images au centre de gestion ou encore le prix du mât sur lequel l'outil peut être installé."*

(…)

DOCUMENT 7

« Les dépôts sauvages dans le viseur des caméras intelligentes » (extrait)

lagazette.fr - publié le 16/09/2024


Mairie de Sète

En moyenne, en France, un habitant abandonne 15 kilogrammes de déchets sauvages par an. Ils génèrent une forte pollution et ont un coût pour les collectivités territoriales. Elles traquent les fauteurs de trouble, qui jettent gravats et encombrants dans la nature en s'équipant de caméras dotées d'intelligence artificielle.

Pas moins d'un million de tonnes d'ordures et d'objets non recyclés, soit l'équivalent de 100 tours Eiffel, sont abandonnés chaque année en France, selon l'association Gestes propres. Partout, en ville comme à la campagne, les déchets sauvages sont devenus un fléau pour les collectivités locales. « Le nombre d'infractions liées aux dépôts de déchets sauvages constatées par la gendarmerie a augmenté de 85 % entre 2017 et 2021. C'est une préoccupation pour 90 % des collectivités territoriales », souligne le Sénat dans un rapport de février 2022 intitulé « Les élus locaux face aux décharges sauvages », qui déplore 36 000 décharges à ciel ouvert dénombrées par l'Agence de la transition écologique.

Un repérage grâce aux mouvements

Si les maires ont l'autorité de police pour lutter contre ce phénomène, l'exercice s'avère de plus en plus difficile, ces derniers s'exposant à des menaces, voire des violences, lorsqu'ils essaient d'intervenir. En 2019, le maire (DVD) de Signes (Var), Jean-Mathieu Michel, 76 ans, avait été renversé et tué par le conducteur d'une camionnette, pris en flagrant délit de dépôt sauvage de gravats. Ce fait divers avait suscité un vif émoi parmi les élus. Depuis la loi « Agec » du 10 février 2020 relative à la lutte contre le gaspillage et l'économie circulaire, les maires disposent toutefois d'un nouveau pouvoir de sanction, avec l'autorisation d'utiliser la vidéosurveillance pour constater des infractions (art. 100) ou identifier des véhicules (art. 101). Désormais, de nombreuses collectivités locales font appel à des caméras de vidéosurveillance intelligentes.

Assis derrière son bureau, Éric Périguey, directeur de la police municipale de Sète (44 700 hab., Hérault), regarde les images de l'une des dix caméras postées depuis le début de l'été à des endroits stratégiques de la ville : « Là, on le voit très bien, un homme vient de déposer des cartons par terre : il y en a plein, et même un tabouret ! ».
Un clic plus tard et le patron de la police municipale récupère la photo de la plaque

d'immatriculation, qui va lui permettre d'identifier très rapidement l'auteur des dépôts de déchets sauvages.

Le principe de ce système développé par l'entreprise Vizzia ? Des caméras autonomes en énergie, mobiles et à double objectif, placées dans des secteurs connus pour leurs dépôts et reliées à la plateforme Vizzia, dont l'algorithme intelligent compare deux images espacées dans le temps et repère, grâce aux mouvements, les dépôts illégaux. L'infraction est enregistrée par une caméra et les images reportées sur un écran. Il suffit ensuite à un agent de les visionner pour constater l'infraction et établir une procédure.

Envoi d'une amende administrative

Après un délai de dix jours, par la voie administrative (art. L. 541-3 du code de l'environnement), le maire peut mettre le propriétaire en demeure d'enlever ses déchets et lui ordonner de payer une amende (15 000 euros maximum). « Là, par exemple, le contrevenant va recevoir, dans les jours à venir, une amende administrative de l'ordre de 250 à 300 euros. Le montant de ces amendes, qui va de 1 000 à 5 000 euros, a été fixé par arrêté municipal et dépend du type et de la quantité de déchets », poursuit Éric Périguey,

L'entreprise Vizzia, qui a de nombreux concurrents (Smart City Mag, Karroad, Acic, etc.), garantit « des résultats exceptionnels » : « quinze détections par caméra en moyenne par mois, une baisse des déchets abandonnés de 80 % en six mois et un coût de collecte et de traitement recouvert à 100 % ».

Pionnière, Montélimar (40 400 hab., Drôme), qui dispose de caméras depuis 2022, se targue d'avoir ramassé « 400 tonnes de déchets sauvages » en 2023. « Le taux de détection est énorme », commente Thierry Lerat, chef de la police municipale [PM]. « Nous sommes prévenus lorsque des dépôts ont eu lieu. Un agent peut alors se consacrer pendant une vingtaine de minutes à l'exploitation des images. L'impunité n'existe plus ». À Sète, en seulement une dizaine de jours, ces dix caméras ont permis aux policiers municipaux de dresser pas moins de cinq amendes. « C'est très efficace », commente Laurence Magne, adjointe au maire (LR) chargée de la propreté. « En matière de déchets sauvages, le flagrant délit est quasi impossible. Avec ces caméras mobiles, nous pouvons faire de la vidéoverbalisation. »

Cependant, si l'investissement peut sembler élevé – 100 000 euros – la ville ne doute pas de le rentabiliser rapidement : « À Sète, nous avons quantifié à 19 kilogrammes par habitant et par jour la quantité de déchets sauvages, alors que la moyenne en Occitanie est de 5 à 6 kilogrammes ! Les enlever est très coûteux », poursuit Laurence Magne. Coercitif, le dispositif se veut aussi préventif. La ville a ainsi envoyé des courriers aux habitants pour les prévenir des risques qu'ils encourent. Elle a aussi revu les horaires de passage des encombrants et multiplie les actions de sensibilisation pour inciter les habitants à jeter leurs déchets à la poubelle et à faire le tri. «L'installation de ces caméras intelligentes s'inscrit dans une politique globale de lutte contre les déchets sauvages, qui mêle sensibilisation et répression. »

Plus besoin de trier parmi des milliers d'images

À Saint-Tropez (3 600 hab., Var), où elles sont installées depuis plus d'un an, ces caméras font aussi l'unanimité. « Le logiciel analyse les images et, tous les jours, nous recevons, dans le respect du règlement général sur la protection des données, celles de dépôts illégaux, avec l'heure, la plaque d'immatriculation, etc.,» explique Thomas Ronsin, responsable de la police de l'environnement. « Concrètement, nous n'avons plus besoin de faire le tri parmi les milliers d'images. »

« Cela nous permet de repérer rapidement le contrevenant », indique le brigadier-chef principal Sylvain Chazal, responsable de la brigade "environnement" de la police municipale de Vernon (24 500 hab., Eure). « S'il vient en véhicule, on va l'identifier et lancer une procédure pour dépôt sauvage. » Hervé Chauvin, le chef de la police municipale, y voit également un même avantage : « L'utilisation de l'intelligence artificielle diminue les heures d'analyse d'images puisqu'on a une alerte lorsque les faits se produisent. C'est un gain de temps. »

Grâce aux caméras, la police de Saint-Tropez identifie, chaque mois en haute saison, quelque 100 à 150 dépôts illégaux. Toutefois, la municipalité, emmenée par Sylvie Siri (DVD), préfère privilégier la sensibilisation. Une fois l'infraction détectée, la police de l'environnement envoie à l'auteur du dépôt sauvage un rapport de constat. Ce dernier dispose alors de dix jours pour entrer en contact avec le service.

« L'auteur peut, durant cette période, nous présenter ses observations », précise Thomas Ronsin. « Si une personne, qui a déposé ses déchets dans les bennes à ordures dédiées, nous explique avoir abandonné un sac sur le parking parce que la benne était pleine, nous allons être indulgents. Nous lui rappellerons juste les règles à appliquer. » Les récalcitrants, eux, se voient infliger une amende administrative qui peut atteindre 15 000 euros.

L'usage est encadré par la loi n°2020-105 du 10 février 2020 modifiant l'article L. 251-2 du code de la sécurité intérieure, ainsi, les dépôts sauvages peuvent être constatés par vidéosurveillance. Cela suppose une autorisation préfectorale qui désigne les agents habilités à exploiter et à visionner les enregistrements en vue d'identifier les auteurs.

(…)

DOCUMENT 8

« Kit caméra de surveillance pour collectivités : guide complet pour choisir et déployer votre système » (extrait)

leaseprotect.fr - 9/12/2024

Face à l'augmentation des incivilités et la nécessité de sécuriser les espaces publics, les collectivités se tournent de plus en plus vers des solutions de vidéosurveillance intelligentes. En 2024, on compte environ 90 000 caméras de vidéoprotection en France. Ce guide vous accompagne dans le choix et le déploiement d'un kit de vidéosurveillance adapté aux besoins spécifiques des collectivités.

Pourquoi installer un kit de vidéosurveillance dans votre collectivité ?

Les collectivités font face à des défis croissants en matière de sécurité publique. Les incivilités, les dégradations et les dépôts sauvages sont autant de problématiques qui nécessitent une réponse adaptée. La vidéosurveillance s'impose comme une solution efficace pour lutter contre ces phénomènes et améliorer la qualité de vie des citoyens.

Selon les dernières statistiques, l'installation de systèmes de vidéosurveillance a permis de réduire significativement les actes de délinquance dans de nombreuses communes. Par exemple, la ville de Nîmes a constaté une augmentation de 23% des amendes en un an grâce à la vidéoverbalisation, démontrant l'efficacité de ces dispositifs.

Il est important de noter que l'installation de caméras de vidéosurveillance est encadrée par un cadre légal strict. La loi de 1995, modifiée à plusieurs reprises, définit les conditions d'utilisation de ces systèmes dans l'espace public. Les collectivités doivent obtenir une autorisation préfectorale et respecter les droits des citoyens en matière de protection des données personnelles.

La vidéosurveillance est devenue un outil incontournable pour assurer la sécurité publique. En 2024, les crédits du FIPDR consacrés à la vidéoprotection vont tripler en 5 ans, témoignant de l'importance accordée à ces dispositifs.

- Diminution des incivilités et des dégradations
- Aide précieuse aux enquêtes en cas d'agressions, vols ou cambriolages
- Dissuasion efficace contre les actes malveillants
- Optimisation de la gestion urbaine (circulation, consommation d'énergie)

Quelle différence entre vidéosurveillance et vidéoprotection pour les collectivités ?

Les termes « vidéosurveillance » et « vidéoprotection » sont souvent utilisés de manière interchangeable, mais ils ont des implications juridiques différentes. La vidéosurveillance fait référence à l'utilisation de caméras dans des espaces privés, tandis que la vidéoprotection concerne les dispositifs installés sur la voie publique par les autorités.

En pratique, cette distinction a des conséquences sur les procédures d'autorisation et les modalités d'exploitation des images. Les systèmes de vidéoprotection sont soumis à un contrôle plus strict et doivent respecter des règles spécifiques en matière d'information du public et de conservation des données.

Le choix entre vidéosurveillance et vidéoprotection dépendra donc des besoins spécifiques de votre collectivité et des zones à couvrir. Il est essentiel de bien définir vos objectifs pour sélectionner le dispositif le plus adapté.

Attention aux restrictions légales

L'utilisation de la vidéosurveillance est strictement encadrée par la loi. Les collectivités doivent veiller à respecter la vie privée des citoyens et à ne pas filmer l'intérieur des habitations. De plus, la CNIL recommande de limiter la durée de conservation des images à 30 jours maximum, sauf cas particuliers.

Comment choisir un kit de vidéosurveillance adapté aux collectivités ?

10 exemples de kits de vidéosurveillance pour collectivités

Pour vous aider à mieux comprendre les options disponibles, voici 10 exemples de kits de vidéosurveillance couramment utilisés par les collectivités :

1. Kit de surveillance des entrées de ville : caméras haute résolution pour lire les plaques d'immatriculation
2. Kit de protection des bâtiments publics : caméras dômes anti-vandalisme pour une couverture à 360°
3. Kit de sécurisation des parcs et jardins : caméras discrètes avec vision nocturne
4. Kit de surveillance des zones commerciales : mélange de caméras fixes et PTZ pour une couverture optimale
5. Kit de vidéoprotection pour petites communes : solution économique avec 4 à 8 caméras
6. Kit de sécurisation des écoles : caméras avec détection de mouvement et alerte en temps réel
7. Kit de surveillance des parkings publics : caméras grand angle avec analyse de flux
8. Kit de protection des zones sensibles : caméras thermiques pour une détection avancée
9. Kit de vidéoverbalisation : caméras haute définition avec zoom optique puissant
10. Kit de surveillance mobile : caméras sur véhicules ou drones pour des événements temporaires

Ces exemples illustrent la diversité des solutions disponibles pour répondre aux besoins spécifiques de chaque collectivité. Le choix du kit dépendra de vos objectifs de sécurité, de votre budget et des particularités de votre territoire.

Quels sont les composants essentiels d'un kit ?

Un kit de vidéosurveillance pour collectivités comprend généralement plusieurs éléments indispensables. Les caméras sont bien sûr au cœur du dispositif, mais elles ne sont pas les seuls composants à prendre en compte. Voici les éléments essentiels à considérer :

- Caméras (dômes, fixes, PTZ)
- Enregistreur vidéo (NVR)
- Disque dur de stockage
- Câbles réseau et alimentation
- Logiciel de gestion et d'analyse

Le choix des caméras est crucial. Il faut opter pour des modèles adaptés aux conditions extérieures, résistants au vandalisme et offrant une qualité d'image suffisante. Les caméras 4K sont de plus en plus prisées pour leur résolution exceptionnelle.

Le stockage des données est un aspect souvent négligé mais essentiel. Il faut prévoir une capacité suffisante pour conserver les images pendant la durée légale, tout en assurant une sécurité optimale des données.

Quelle technologie privilégier ?

Le choix de la technologie dépendra de vos besoins spécifiques et de votre budget. Les systèmes IP sont aujourd'hui largement répandus et offrent de nombreux avantages en termes de qualité d'image et de flexibilité. Cependant, les solutions analogiques peuvent encore être pertinentes dans certains cas, notamment pour des budgets plus restreints.

Les solutions sans fil gagnent du terrain, notamment pour éviter des travaux de génie civil coûteux. Elles offrent une grande flexibilité d'installation mais nécessitent une attention particulière à la sécurité des transmissions.

L'intelligence artificielle révolutionne le domaine de la vidéosurveillance. Des outils comme LPPredict de Lease Protect France permettent une analyse en temps réel des images pour détecter automatiquement les comportements suspects. Cette technologie améliore considérablement l'efficacité des systèmes en réduisant les faux positifs et en facilitant le travail des opérateurs.

Comment fonctionne un système de vidéosurveillance sans wifi ?

Les systèmes de vidéosurveillance sans wifi utilisent généralement des technologies alternatives pour transmettre les données. Les solutions les plus courantes sont :

- La transmission par câble Ethernet (PoE)
- Les réseaux cellulaires 4G/5G
- Les liaisons radio propriétaires

Ces solutions offrent l'avantage d'être moins vulnérables aux interférences et aux piratages que le wifi. Elles sont particulièrement adaptées pour couvrir de grandes zones ou des sites isolés.

Pour les collectivités, les systèmes sans wifi présentent plusieurs avantages. Ils sont généralement plus fiables et offrent une meilleure qualité de transmission sur de longues distances. De plus, ils permettent de s'affranchir des contraintes liées à l'installation et à la maintenance d'un réseau wifi étendu.

Comment installer et gérer un kit de vidéosurveillance ?

Quelle est la procédure d'installation ?

L'installation d'un système de vidéosurveillance dans une collectivité nécessite une planification minutieuse. Voici les étapes clés à suivre :

1. Réalisation d'un audit de sécurité
2. Obtention des autorisations nécessaires
3. Choix de l'emplacement des caméras
4. Installation du matériel
5. Configuration du système
6. Tests et mise en service

Il est crucial de respecter les normes en vigueur, notamment en matière d'affichage et d'information du public. Une attention particulière doit être portée à la sécurisation du réseau et des données collectées.

- Vérifier la conformité légale
- Tester la qualité des images de jour comme de nuit
- Former le personnel à l'utilisation du système
- Mettre en place des procédures de sauvegarde des données
- Prévoir un plan de maintenance régulière

Comment assurer la maintenance ?

La maintenance d'un système de vidéosurveillance est essentielle pour garantir son efficacité dans la durée. Une maintenance préventive régulière permet de détecter et de corriger les problèmes avant qu'ils n'affectent le fonctionnement du système. Cela inclut le nettoyage des caméras, la vérification des connexions et la mise à jour des logiciels.

En cas d'incident, il est important d'avoir mis en place des procédures claires pour une intervention rapide. Des outils comme LPSurvey de Lease Protect France permettent une détection en temps réel des dysfonctionnements, facilitant ainsi la maintenance corrective.

La formation des agents est un élément clé pour tirer le meilleur parti de votre système de vidéosurveillance. Des opérateurs bien formés peuvent faire la différence entre un système efficace et un investissement sous-exploité.

(...)

DOCUMENT 9

« Vidéosurveillance intelligente : les usages controversés du logiciel Briefcam »

lagazette.fr - publié le 08/01/2024

Une centaine de villes en France utiliseraient aujourd'hui le logiciel d'analyse d'images Briefcam, au centre d'une polémique depuis la publication d'un article sur son utilisation dans la police nationale. Explications.

A la lumière de la récente jurisprudence administrative, l'utilisation de Briefcam se révèle désormais au grand jour. Après une première injonction à cesser le recours à ce logiciel de vidéosurveillance automatisée et deux rejets prononcés par des tribunaux administratifs, le Conseil d'Etat vient finalement de donner un premier "la" juridique, le 21 décembre dernier.

La plus haute juridiction de l'ordre administratif a finalement donné raison à la communauté de communes cœur Côte Fleurie (Calvados). Faute de situation d'urgence particulière, l'ordonnance du juge des référés du tribunal administratif de Caen a été retoquée. Quasiment un mois plus tôt, le 22 novembre, ce dernier avait enjoint la collectivité territoriale à arrêter son utilisation du logiciel Briefcam et à effacer les données collectées en raison "des risques pour les droits et libertés fondamentaux des personnes et la préservation de leur anonymat".

Plaques d'immatriculation et statistiques

Autant de procédures qui ont permis d'en savoir plus sur l'usage réel de ce logiciel par les collectivités territoriales. La CC cœur Côte Fleurie a ainsi assuré ne pas pouvoir – ni vouloir – mettre en œuvre la controversée fonctionnalité du logiciel : la reconnaissance faciale. Ce fragile programme – il n'est plus en état de marche à la suite des opérations effectuées après la première ordonnance – sert plutôt à compter les flux de circulation sur les grands axes routiers et à répondre aux réquisitions judiciaires à des fins de recherche de plaques d'immatriculation.

A Nice (Alpes-Maritimes), le juge des référés remarquait que le logiciel avait seulement été utilisé à titre expérimental lors de l'Euro 2016 de football et du carnaval en 2019. La ville de Roubaix (Nord) avait également signalé ne pas avoir activé la fonction de reconnaissance faciale. Elle précisait à la justice administrative n'utiliser le logiciel que pour des recherches a posteriori de plaques d'immatriculation sur réquisition judiciaire. Soit, en tout, seulement 23 recherches au cours de l'année écoulée, une utilisation validée par la Cnil lors d'un contrôle en avril 2023.

Booster ou fuite en avant ?

Selon ses partisans, l'utilisation des algorithmes pour détecter des objets ou des comportements suspects est censée booster la vidéosurveillance. Ce type de logiciel est généralement vendu aux collectivités territoriales moyennant « un forfait annuel d'une centaine d'euros à 1 000 euros par caméra », compte François Mattens,

directeur des affaires publiques de XXII, une société française spécialisée dans l'analyse vidéo.

Ses détracteurs estiment au contraire qu'il s'agit avant tout de la fuite en avant technologique d'une solution sécuritaire qui n'a toujours pas démontré son efficacité. Un débat ancien ravivé par un article de Disclose. A la mi-novembre, le média d'investigation signalait qu'une centaine de villes en France utilisaient Video Synopsis, son programme d'analyse d'images.

Mais Disclose pointait surtout une utilisation illégale depuis 2015 par la police nationale. Ce même logiciel permettrait d'analyser les visages, alors que le recours à la reconnaissance faciale vient d'être écarté pour les Jeux olympiques et paralympiques de Paris 2024. Dans la foulée, la Cnil annonçait le lancement d'une procédure de contrôle du ministère de l'Intérieur, tandis que le locataire de la Place Beauvau, Gérald Darmanin, demandait une enquête administrative interne.

Fausses alertes

Cette controverse avait entraîné le lancement de plusieurs actions en référé contre des collectivités territoriales. Elles étaient portées par la Ligue des droits de l'homme, le Syndicat de la magistrature, l'Union syndicale Solidaires, l'Association de défense des libertés constitutionnelles et le Syndicat des avocats de France. Ces organisations pointaient dans leur recours une dissimulation de l'usage, par des collectivités territoriales, de cette solution basée sur l'intelligence artificielle. Elles s'inquiétaient également des risques d'atteinte grave au respect de la vie privée, par exemple en identifiant des personnes physiques grâce à leurs vêtements ou en les suivant de manière automatisée.

Controversée, cette technologie doit encore faire ses preuves. A Perpignan (Pyrénées-Orientales), le logiciel n'a ainsi qu'une poignée d'usages, assure à « La Gazette » Philippe Rouch, autour du comptage de personnes lors de manifestations ou de véhicules sur la voirie. « Je voulais m'en servir pour repérer les dépôts sauvages, mais cela ne marche pas, la technologie n'est pas encore au point », remarque le directeur de la police municipale. « En démonstration, cela marche très bien. Mais quand on l'utilise vraiment, il y a plein de fausses alertes et cela détourne l'attention de l'opérateur. »

« Sécurisation d'un réseau informatique dédié à la vidéoprotection. Systèmes et contrôle » (extraits)
dumas.ccsd.cnrs.fr - 29/11/2021

(…)

2.3.3. Socle de sécurité

Au regard du périmètre métier et technique de l'étude, les référentiels suivants ont été retenus pour établir le socle de sécurité du système :

Tableau VIII : Liste des référentiels applicables

Id	Référentiel	Rédacteur	Version
Réf 1	Guide d'hygiène informatique	ANSSI	2.0
Réf 2	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection	ANSSI	2.0
Réf 3	Référentiel APSAD D32 Cybersécurité	APSAD	Juin 2017

Le guide d'hygiène informatique de l'ANSSI [ANSSI - 2017] a été publié initialement en 2013 et mis à jour en 2017. Il décrit un ensemble de mesures de sécurité applicables aux systèmes d'information en général. Ces mesures sont issues de l'expérience de l'ANSSI en fonction des constats fait lors de ses différentes interventions à la suite d'attaques informatiques. L'ANSSI part du principe que si les mesures que ce référentiel décrit avaient été appliquées, la majeure partie de ces attaques auraient pu être évitées. Le guide énumère 42 mesures de sécurité d'ordres organisationnelles ou techniques. Elles seront retenues en fonction de leurs pertinences et applicabilités à l'objet de l'étude.

Le guide de recommandation sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection [ANSSI - 2020a] , également publié par l'ANSSI, dresse quant à lui des mesures de sécurité spécifiquement étudiées pour ces systèmes. Sa version initiale date de 2012 et il est actuellement dans sa version 2.0 datant de mars 2020. Les mesures de sécurité listées sont au nombre de 91, mesures qui seront également retenues en fonction de l'objet de l'étude.

Le Centre National de la Prévention et de la Protection (CNPP), qui délivre les certifications APSAD, a également publié un guide traitant de la cybersécurité des systèmes de sécurité, le référentiel D32 [CNPP - 2017]. Les certifications APSAD sont délivrés aux entreprises installant des systèmes de sécurité (R81 pour les systèmes de détection intrusion, D83 pour les systèmes de contrôle d'accès, R82 pour les systèmes de vidéoprotection) et sont gages de qualité dans l'installation de ces systèmes. L'entreprise Securitas Sécurité Electronique étant

déjà certifiée APSAD R81, R82 et D83, il est tout naturel que les systèmes qu'elle installe suivent les recommandations du référentiel en vue d'être à l'avenir certifié APSAD D32.
Les mesures de sécurité listées dans ces documents sont de trois types :

- Organisationnelles : ces mesures seront mises en place par l'organisation en établissant des procédures spécifiques, des chartes ou des règles d'utilisation informatique, des formations techniques ou de sensibilisation de ses collaborateurs. Il s'agit également de mettre en place une démarche d'amélioration continue de la sécurité du système d'information, en planifiant des audits réguliers et des mises à jour du système en conséquence.

- Physiques : les mesures de sécurité physiques s'appliqueront sur les modes d'installation ou de protection physique des composants du système d'information, comme par exemple le fait d'installer les éléments clés du système d'information (serveurs, commutateurs, systèmes de sauvegarde…) dans les locaux protégés aux accès limités.

- Techniques : les mesures techniques seront quant à elles appliquées par l'utilisation de matériels ou logiciels spécifiques, du durcissement de la configuration des équipements et de l'utilisation de protocoles sécurisés.

(...)

DOCUMENT 11

« L'installation d'un système de vidéosurveillance » (extrait)

telesurveillance-videosurveillance.fr - 17/12/2025

L'installation d'un **système de vidéosurveillance** se base sur 3 étapes fondamentales : la réception, la gestion et la visualisation des images et ce quel que soit le système que vous choisissez (analogique, numérique, IP…). Cette installation peut être réalisée par un professionnel, généralement le fournisseur qui vous a vendu le matériel, ou bien vous pouvez installer votre système vous-même. Toutefois, il est recommandé de confier cette tâche à un spécialiste, vous avez de cette manière une garantie quant à la qualité de l'installation, de la configuration et au fait que votre **système de vidéosurveillance** est tout de suite opérationnel.

Quel que soit votre choix, installateur professionnel ou pas, voici un aperçu des étapes nécessaires à sa mise en place et des choix que vous devez faire en amont.

Système de vidéosurveillance, le préambule à toute installation

Avant toute installation, il convient de réaliser une étude des besoins afin que le **système** choisi corresponde à vos besoins. C'est lors de cette étude, réalisée par un expert, que plusieurs éléments doivent être déterminés :

- Zones stratégiques à surveiller,
- Type de caméras à installer,
- Positionnement des caméras (étape essentielle pour des caméras sur un réseau câblé),
- Emplacement de la régie vidéo ou poste de contrôle…

Cette étude est indispensable avant toute installation de système de surveillance. Elle évite les mauvaises surprises. Pour trouver un spécialiste, n'hésitez pas à réaliser plusieurs demandes de devis. De cette façon, vous pouvez avoir plusieurs avis d'experts et comparer les offres.

Les différentes architectures d'une installation

Pour un **système de vidéosurveillance**, vous avez deux possibilités : l'installation en circuit fermé ou en circuit ouvert.

Le principe d'un système en circuit fermé, appelé aussi CCTV (Closed Circuit Television) est de relier sur le même réseau interne à une structure (entreprise, établissement…) des caméras, un ou plusieurs moniteurs et éventuellement un enregistreur. Ce type d'installation est valable pour les professionnels ne souhaitant pas diffuser en temps réel les images en dehors de l'entreprise à l'inverse de la visualisation à distance. Le CCTV est, historiquement, le premier système de vidéosurveillance mais il s'est bien amélioré depuis avec l'utilisation de matériels de plus en plus complexes : caméras en couleur, enregistreur DVD…

A l'inverse, un système en circuit ouvert ou OCCTV est un système connecté à un réseau extérieur : internet. Ce procédé permet l'accès à de nombreuses fonctionnalités : surveillance de locaux à distance, télésurveillance, surveillance multi-sites… Ce type d'installation a vu le jour avec le développement d'internet et notamment du haut débit. Il connaît encore des évolutions avec l'arrivée des smartphones, de la fibre optique…

Les éléments matériels à installer pour votre système de surveillance vidéo

Celui-ci doit comprendre au minimum :

- Une ou plusieurs caméras couvrant les zones que vous souhaitez surveiller,
- Un appareil de gestion des images : ordinateur, commutateur, logiciel…
- Un moniteur pour la visualisation des images.

Vous pouvez également ajouter un appareil d'enregistrement tel qu'un magnétoscope ou un enregistreur numérique et remplacer le moniteur par l'écran d'un ordinateur ou d'un Smartphone. Les possibilités sont nombreuses, c'est pourquoi il est recommandé de demander conseil à son fournisseur ou à des prestataires en vidéosurveillance.

D'un point de vue technique, pour installer vos caméras IP vous devez :

- donner une adresse IP à la caméra ou au serveur de caméra,
- assurer la configuration des caméras depuis un navigateur car elle doit se faire en HTTP. La caméra est comme tout serveur internet, on s'y connecte via un ordinateur et on la configure grâce aux différents menus disponibles.

Une fois tous les éléments connectés et les configurations correctement effectuées, votre système de surveillance est prêt à fonctionner !

(…)