Pourquoi l'AIPD (étude d'impact relative à la protection de données) occupe-t-elle aujourd'hui une place si critique dans tout projet de vidéoprotection (installation, extension, changement de type de capteur)?

…et pourquoi tous les élus comme leurs équipes doivent s'en préoccuper et veiller à leur mise à jour.

Lors des dernières élections municipales, la sécurité du quotidien a souvent occupée une place importante pendant la campagne – à tort ou à raison. S'il n'y a pas eu (ou très rarement) de débats relatifs au principe même d'une vidéosurveillance (ou vidéoprotection), le plus souvent les candidats ont annoncé une extension des systèmes existants, voire un renforcement de « l'efficacité opérationnelle » de ces réseaux en faisant appel « aux nouvelles technologies » (l' intelligence artificielle, IA), mais en étant rarement très explicite…

1 Un cadre juridique qui a été récemment précisé avec des obligations qui ne doivent pas être prises à la légère

Dorénavant, la mise en œuvre de ces engagements repose sur de nouveaux élus : des maires ont changé et même si la stabilité politique a prévalu, en revanche ce sont souvent des équipes remaniées, rajeunies qui sont en place.

Or, par rapport aux élections de 2020, d'une part les techniques ont évoluées (désormais on parle couramment de VSA comme vidéoprotection intelligente ou augmentée ou algorithmique avec des caméra voire les systèmes d'exploitation équipés de couches d'IA) et celles-ci sont « vendues » et leur efficacité promue par un écosystème d'entreprises bien organisé, dont la conformité au cadre juridique n'est pas la préoccupation première.

D'autre part, le cadre normatif applicable -déjà très complet au sein du CSI[1] et de la loi 78-17 modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (intégrant le « paquet européen » de 2016 -règlements RGPD et « Police-justice ») – a été assez récemment précisé par des jurisprudences (2025 et 2026) des juridictions administratives, par des sanctions assorties d'

[1] Code de la sécurité intérieure (CSI)

explications prises par la CNIL depuis fin 2024, l'ensemble étant éclairé par la prise de position du Conseil Constitutionnel saisi en 2023[2] de la loi du 19 mai 2023 relative aux JOP 2024 qui comportait un dispositif expérimental original très complet de traitement d'images.

Le non-respect de ce cadre peut entrainer des sanctions pécuniaires non négligeables pour les collectivités (prononcées par la CNIL), des contentieux à forte résonnance médiatique et réputationnelle (surtout si des collectifs citoyens ou ONG spécialisées les ont initié) voire des difficultés lourdes avec la commission départementale de vidéoprotection (présidée par un magistrat et habilitée à procéder à des contrôles), la CNIL (qui agit sur plainte, signalement ou dans le cadre d'un contrôle) et du préfet. Il a été rappelé aux préfets par circulaires du 20 mars 2024[3] relative à « la mise en conformité du régime de la vidéoprotection avec le droit européen relatif à la protection des données » et du 16 avril 2024 [4]« ..portant sur l'habilitation du personnel des collectivités territoriales et de leurs groupements procédant au visionnage des images de vidéoprotection » qu'ils pouvaient diligenter les contrôles par les services de police/gendarmerie portant sur la conformité des système et l'utilisation de systèmes non autorisés. Ces contrôles peuvent déboucher sur une suspension de l'autorisation d'exploiter, un retrait d'autorisation et pour les cas les plus graves une fermeture temporaire voire définitive de l'établissement. Les termes de cette circulaire sont suffisamment clairs et précis pour que ce risque – jusqu'à peu assez théorique- soit clairement identifié dorénavant par les responsables des traitements.

2 Des élus et des collectivités souvent confrontés à des problèmes complexes et en interne, un manque d'expertise à la fois règlementaire et opérationnelle

D'autre part, ces nouveaux élus sont confrontés aujourd'hui à plusieurs problèmes. Le parc de caméras installées sur la voie publique s'élève à quelques 115 000 (chiffre vraisemblablement très sous-estimé), auxquelles s'ajoutent plus de 200 000 à l'extérieur d'établissements ouverts au public- façades, parcs, parkings ouverts au public- et un peu plus de 800 000 à l'intérieur d'établissements ouverts au public-galeries marchandes, musées, enceintes sportives et lieux culturels ; comme pour l'essentiel il s'agit de réseaux municipaux (plus rarement privés), les élus sont confrontés à un problème

[2] Décision 2023-850 DC du 17 mai 2023
[3] Reference : NOR : IOMD2405307J . Circulaire publiée
[4] Reference : NOR : IOMB2403160C. Circulaire publiée

capacitaire. Dans le millier de CSU[5] qui pilotent ces réseaux urbains, il y a un enjeu d'efficacité et d'automatisation du travail des opérateurs (question de l'attention « physique » des opérateurs qui visionnent en temps réels de très nombreuses caméras). La contrainte budgétaire rend peu envisageable l'embauche de plus d'opérateurs pour surveiller H24 un tel parc d'autant plus que n'importe quel spécialiste qui a vu fonctionner un CSU sait que la tâche s'apparente le plus souvent à l'attente décrite dans le désert des tartares par D Buzatti.

Donc il est important pour tout nouvel élu d'acquérir une vision globale, préalable au lancement de ces nouveaux équipements, confrontés qu'ils sont aux promesses technologiques que font miroiter les industriels et aux cûts de ces systèmes (une caméra « actuelle » de VSA peut atteindre 20 000€ aujourd'hui contre 4000 en 2020 et les coûts de maintenance des systèmes exposent) , aux éventuelles conséquences d'un contrôle diligenté par l'Etat et aux attentes de leurs agents employés dans les CSU.

3 Qu'est qu'une AIPD ? Ce qui est permis et prohibé ?

A- L'AIPD (sommairement) : ce que ça n'est pas et ce que c'est réellement !

En premier lieu, on ne doit pas confondre une AIPD avec le document stratégique d'une municipalité en matière de sécurité , et l'AIPD ne constitue en aucun cas le « levier stratégique » d'une installation de vidéoprotection, comme on peut le lire chez certains industriels du secteur. Et si c'est le cas, alors la collectivité a pris son projet complètement à l'envers !

Il revient aux élus après débat au sein des instances ad hoc (commission, conseil municipal) de s'accorder sur deux principes « opératifs » avant de lancer tout projet de création/ extension/ modernisation en se posant les questions fondamentales, au regard de leurs compétences légales et des moyens engagés (CSU et coordination opérationnelle au sein de la police municipale et surtout avec la police nationale qui a des compétences plus larges et de de nature judiciaire- le projet de loi police municipale attendu pour cet automne n'y changera rien !) : **quel est l'effet que la collectivité souhaite atteindre ?** et **comment sont évalués les résultats au regard des objectifs qu'elle s'est fixés ?** Dès lors que des réponses politiques claires sont apportées, la seconde chose à faire est de mettre au point et surtout formaliser une **doctrine d'emploi**

[5] CSU : centre de supervision urbaine

opposable, propre à la police municipale et au système de videoprotection (chef de salle du CSU en fonction des consignes du maire ou élu en charge de la sécurité/sureté).

A titre d'illustration, il est rappelé, notamment, que l'analyse en temps réel de vidéo enregistrées dans l'espace public, tout comme l'identification des visage est interdite (sauf pour certains services de l'Etat et dans un cadre juridique spécifique) mais qu'en revanche, l'analyse automatisée a posteriori est autorisée sous certaines conditions (règlement européen « police-justice ») en particulier dans le cadre d'enquêtes judiciaires et par des OPJ sous le contrôle d'un juge. Or, des logiciels proposés aux collectivités permettent d'accéder à distance à des images enregistrées et stockées sur des serveurs de la collectivité (voire de cloud) et d'y opérer des recherches poussées avec comme argument de vente que « cela permet un accès à la preuve instantanée et d'espérer accélérer ainsi les échanges entre agents municipaux et les forces de l'ordre ». Ces « dérives » observées dans plusieurs collectivités doivent pouvoir être précisées et encadrées dans une doctrine d'emploi, par exemple.

Pourquoi, précise-t-on la nécessité de ces deux étapes : d'une part, parce qu'elles ne sont pas pratiquées ou très peu dans les collectivités- la vidéoprotection est trop souvent une orientation prise sous pression électorale sans une analyse de fond bien objectivée des besoins des habitants- et d'autre part, parce que les choix techniques et partant l'AIPD – document crucial pour les instances de contrôle- seront plus aisés à rédiger et à expliquer (question de la légitimité du projet, de la proportionnalité des moyens déployés, explication de la conformité etc…). Accessoirement, on peut mesurer plus aisément l'adéquation du projet déployé avec l'enveloppe budgétaire et la capacité RH de la collectivité…

En second lieu, une AIPD est un document principalement juridique, dont les rubriques sont assez normées par les exigences du cadre européen : c'est une analyse d'impact relative aux données « brassées » par un système de capture et de traitement de données personnelles -ici des images prises sur l'espace public. Un tel dispositif est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques. La rédaction d'un tel document est obligatoire (en France comme au sein de l'UE) dans l'hypothèse ou le dispositif envisagé présente un risque sérieux d'atteinte aux droits et libertés des personnes. Cette obligation n'est pas applicable en matière de défense

nationale. Pour savoir si une AIPD est nécessaire, il convient de se référer à une grille de **9 critères** établis par la CNIL[6] : dans la plupart des cas, un responsable de traitement peut considérer qu'un dossier satisfaisant à 2 critères nécessite une AIPD et d'une manière générale, plus le traitement cumule de critères de cette grille, plus il est susceptible de présenter un risque juridique élevé pour les droits et libertés des personnes concernées et donc de nécessiter une AIPD de plus en plus solide.

La doctrine de la CNIL est simple, lisible (il faut souligner les efforts pédagogiques constants de l'autorité : de manière schématique la CNIL considère qu'est prohibé tout ce qui ne lui parait ni légitime, ni proportionné. Aussi dans la majorité des cas (notamment les petites installations), l'AIPD sera plutôt un exercice utile mais qui demeure raisonnable et léger dans la majorité des situations. En revanche, avec des couches d'IA embarquées sur les capteurs (caméras « intelligentes ») ou sur les serveurs avec des algorithmes de recherche- outils **couramment vendus sur le marché aujourd'hui** , on change la nature du risque juridique car ce ne sont plus des caméras qui enregistrent mécaniquement mais derrière c'est désormais un système entier qui analyse, interprète, alerte plus ou moins automatiquement !

C'est la raison pour laquelle, il est conseillé au regard de la complexité méthodologique de l'exercice (porté par une gouvernance interne complexe avec des élus, un administratif en charge de la sécurité, une structure en charge des systèmes d'information voire le RSSI et si besoin le Délégué à la protection des données- DPO), de se faire assister par un avocat. Ce professionnel du droit, qui offre de solide garanties de compétences et de responsabilité, a l'habitude d'internaliser cette complexité structurelle : identification des risques, qualification juridique de ceux–ci, formalisation des mesures voire accompagnement de la mise en œuvre de celles-ci (explication pédagogique, formation…). C'est avant tout une expertise réglementaire et opérationnelle – les choix techniques, contrairement à ce que les « spécialistes » annoncent, jouent un rôle finalement assez secondaire- car il s'agit ici de manier des principes juridiques (peser la justification de la légitimité ou la notion de proportionnalité) et de déployer des mesures opérationnelles de bon sens afin que les élus puissent communiquer auprès de leurs administrés tout comme les organismes de contrôle. Enfin, l'AIPD ne doit pas être conçue comme un document statique car elle implique une démarche continue intégrée au cycle

[6] Voir le site de la CNIL : http://www.cnil.fr/RGPD-analyse-impact6protection -des-données-aipd

de vie (et des usages y compris à venir) des installations : cette dimension doit être intégrée dans le document.

Selon la nature de l'installation et des AIPD à rédiger (voire à présenter devant la CNIL- ses services et/ou les conseillers- s'il s'agit d'un dossier sensible) le cout peut varier (aujourd'hui) entre 5 à 6000€ mais entre 3 à 4 fois plus pour les dossiers les plus complexes et lourds. Mais pour relativiser, un capteur très performant dernier cri équipé de couches d'IA embarquées atteint aujourd'hui quelques 20 000€ !

B- Le rappel aux règles fondamentales : les 8 usages de l'IA prohibés en Europe

Il est utile de rappeler que la Commission européenne avait précisé début 2025 les 8 usages de l'IA désormais prohibés dans l'UE car jugés dangereux :

-identification en temps réel de personnes à l'aide de caméras dans les lieux publics. C'est le rappel de la prohibition de la reconnaissance faciale en temps réel (permise toutefois dans le cadre du règlement « police-justice » mais pour des missions des forces de l'ordre) ;

-notation sociale à partir de données personnelles sans lien avec le risque évalué ;

-évaluation du risque criminel d'un individu sur la base de données biométriques ;

-créer des bases de données (d'entrainement à grande échelle) des visages pour des systèmes de reconnaissance faciale en récupérant des images sur internet ;

-reconnaissance des émotions sur le lieu de travail ou des institutions éducatives ;

-manipuler le comportement des individus à l'aide de l'IA ;

-manipuler le comportement des individus à l'aide de l'IA ;

-exploiter les vulnérabilités liées à l'âge ou au handicap ;

-déduire les opinions politiques ou l'orientation sexuelle en fonction de données biométriques.

En outre, la CNIL a de son côté rappelé fin mars 2026, de manière ferme, non seulement le cadre légal de la vidéoprotection mais aussi l'interdiction absolue de l'enregistrement sonore direct par un système couplé avec celui de la vidéo

protection (microphones intégrés aux caméras). Ce type d'enregistrement demeure autorisé dans les établissements publics ou privés recevant du public : mais c'est un dispositif autonome de la vidéoprotection, non automatisé et qui enregistre ponctuellement, en cas de danger, agression. Elle n'a jamais manqué de rappeler que d'autres usages étaient proscrits tel [aujourd'hui] la lecture automatique des plaques (LAPI), la détections d'auteurs de dépôts sauvages de déchets, la remontée d'alerte quand un groupe de personne se promène, se forme ou chahute ou encore la captation d'informations liées à certains comportements…car ceci peut s'inscrire dans un processus de surveillance de masse.

Pour conclure, si l'AIPD s'impose en 2026 comme une étape cruciale de tout projet de vidéoprotection et non une énième obligation normative, c'est que d'une part , le cadre juridique issu du « paquet européen » de 2016 (transposé il est vrai en 2018) n'est toujours pasvraiment intégré dans les obligations des communes et d'autre part, que maints acteurs du marché sont défaillants dans leur devoir de conseil et que certains prestataires n'hésitent pas à déployer des solutions qui promettent n'importent quoi, à la limite de la légalité ! Il faut donc se mettre en accord avec ce cadre juridique qui n'est en rien insurmontable, mais ne pas hésiter à s'adresser à des professionnels du droit car l'AIPD n'est en rien un document technique mais bien la charte juridique et des usages opérationnel d'une installation de vidéoprotection dont se dote une collectivité et son équipe dirigeante.

Juin 2026

Jean-christophe Moraud