Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2024

ÉPREUVE DE PROJET OU D'ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription.

Durée : 4 heures
Coefficient : 5

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION
OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

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 54 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 répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes ingénieur territorial, chargé de mission du numérique au sein de la communauté d'agglomération INGEAGGLO (80 000 habitants). Vous êtes directement rattaché au Directeur Général des Services (DGS).

INGEAGGLO a fait de la question du développement du numérique sur l'ensemble de son territoire une priorité. Elle va lancer prochainement un schéma directeur de développement du numérique en relation étroite avec l'ensemble des communes qui la composent, dans une logique de mutualisation des moyens et d'efficacité des services à déployer.

La transformation numérique au sein d'INGEAGGLO est cependant déjà amorcée au travers d'une demande politique forte liée au développement d'un système de vidéoprotection organisé à l'échelle de l'EPCI et centralisé autour d'un Centre de Supervision Urbain (CSU). Actuellement, seules quelques initiatives ponctuelles ont été menées par certaines communes, sans concertation et sans réelle cohérence.

Question 1 (4 points)

Dans le cadre de l'étude préalable au schéma directeur de développement du numérique, vous préciserez les objectifs et les enjeux de la transformation numérique notamment au regard des différentes démarches de dématérialisation déjà initiées par l'Etat et les collectivités territoriales.

Question 2 (4 points)

La vidéoprotection mutualisée étant une demande prioritaire des élus, le Président d'INGEAGGLO vous demande, sous couvert du DGS, de lui faire parvenir une note lui permettant d'apprécier l'intérêt et la pertinence d'une mutualisation sur ce type de projet ainsi que les contraintes et les limites qui en découlent.

Question 3 (4 points)

L'avènement de l'Intelligence Artificielle (IA) permet d'envisager de nouvelles perspectives en matière de vidéoprotection avec la mise en œuvre de systèmes toujours plus innovants mais qui peuvent susciter également des craintes. De nombreuses expérimentations sont actuellement menées en ce sens sur des systèmes de vidéoprotection augmentés par l'IA.

Le DGS vous demande de rédiger un ensemble de propositions opérationnelles et de recommandations dans le cadre de la mise en œuvre d'une expérimentation de ce type de dispositif au sein d'INGEAGGLO.

Question 4 (3 points)

INGEAGGLO ne disposant pas d'un réseau complétement irrigant sur l'ensemble de son territoire, il apparait nécessaire d'associer à l'existant des capacités offertes par d'autres technologies et capables de s'intégrer aux réalisations actuelles.

Parmi ces nouvelles technologies, la 5G constitue une évolution technique pertinente. Vous expliciterez en quoi cette technologie pourrait représenter une opportunité pour le projet de vidéoprotection d'INGEAGGLO.

Question 5 (5 points)

La mise en place d'un système de vidéoprotection mutualisé est complexe et nécessite de bien définir les différentes phases à mener. Les questions de la temporalité et de la communication à prévoir auprès des différents publics cibles sont importantes.

Votre DGS vous demande de lui proposer une démarche concertée détaillant les principales étapes à conduire pour mener à bien ce projet.

Liste des documents :

Document 1 : « Une circulaire pour mettre en œuvre la vidéoprotection mutualisée » - *La Gazette des communes* - 15 mars 2022 - 2 pages

Document 2 : « Caméras dites « augmentées » dans les espaces publics : la position de la CNIL » - *CNIL* - juillet 2022 - 4 pages

Document 3 : « Vidéoprotection : La CNIL rappelle le cadre juridique aux collectivités » - *infos.haas-avocats.com* - 12 janvier 2022 - 3 pages

Document 4 : « Intelligence artificielle : le plan d'action de la CNIL » - *CNIL* - 16 mai 2023 - 5 pages

Document 5 : « Comment les industriels de la vidéosurveillance imaginent le futur » - *La gazette des communes* - 31 mars 2022 - 2 pages

Document 6 : « Collectivités territoriales : des sénateurs préconisent des mutualisations dans la vidéosurveillance et la cybersécurité » - *Label Résiliance France Collectivités* - 20 janvier 2022 - 2 pages

Document 7 : « Les enjeux de la transition numérique au sein des collectivités » - *Nepsio Conseil* - 26 avril 2022 - 3 pages

Document 8 : « Dans les collectivités, la transition numérique repose aussi sur la maîtrise de compétences numériques » - *Caissedesdepots.fr* - 24 janvier 2022 - 4 pages

Document 9 : « Le défi de la digitalisation des collectivités territoriales » - *solocal.com* - 15 novembre 2022 - 4 pages

Document 10 : « Mutualisation de la vidéoprotection : une instruction pour veiller à la bonne mise en œuvre de la loi Sécurité globale » - *Localtis* - 28 mars 2022 - 2 pages

Document 11 : « Surveillance vidéo des lieux publics : comment adapter le cadre juridique ? » - *Viepublique.fr* - 19 avril 2023 - 2 pages

Document 12 : « Vidéosurveillance IA : un dispositif déployé dans toute la France après les JO ? » - *lebigata.fr* - 26 septembre 2023 - 2 pages

Document 13 : « La méthode agile expliquée de A à Z pour faire avancer vos projets avec souplesse » - *appvizer.fr* **-** 16 juin 2022 - 3 pages

Document 14 : « Toulouse : comment la ville renforce son arsenal de vidéoprotection » - *Ladepeche.fr* - 14 juillet 2021 - 2 pages

Document 15 : « COMINFOS: IOT, Vidéoprotection, Edge computing, 5G, si nous en parlions de façon simple… » - *Groupe Videocom* - 16 mars 2023 - 3 pages

Document 16 : « Directive NIS 2 : ce qui va changer pour les entreprises et l'administration françaises » - *ANSSI* - 13 octobre 2023 - 3 pages

Document 17 : « I Act : une régulation européenne tout en compromis » - *lemondeinformatique.fr* - 11 décembre 2023 - 1 page

Document 18 : « Sécurité : Protéger le réseau informatique interne » - *CNIL* - 5 mai 2023 - 2 pages

Liste des annexes :

Annexe A : « Présentation d'INGEAGGLO » - *INGEAGGLO* - 2023 - 1 page

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

La Gazette des communes - 15 mars 2022

Une circulaire pour mettre en œuvre la vidéoprotection mutualisée

La loi sécurité globale du 25 mai 2021 élargit les possibilités de mutualisation pour installer et entretenir un dispositif de vidéoprotection. L'instruction parue le 4 mars 2022 en explicite la mise en oeuvre.

L'article 42 de la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés a prévu de nouvelles possibilités pour les collectivités territoriales et leurs groupements d'acquérir, d'installer et d'entretenir des dispositifs de vidéoprotection mutualisés.

Une instruction du 4 mars explicite la façon dont les collectivités territoriales et leurs groupements peuvent mettre en œuvre des systèmes de vidéoprotection à la suite de ces nouvelles dispositions.

Des finalités définies

Le gouvernement rappelle d'abord le cadre réglementaire. L'article L. 251-2 du code de la sécurité intérieure (CSI) prévoit que la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes pour l'une ou plusieurs des onze finalités prévues par ces dispositions :

- la protection des bâtiments et installations publics et de leurs abords ;
- la régulation des flux de transport ;
- la constatation des infractions aux règles de la circulation ;
- la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ;
- la prévention des risques naturels ou technologiques ;
- le secours aux personnes et la défense contre l'incendie ;
- la prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets ;
- etc.

De même, un système de vidéoprotection peut également être déployé dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.

Les personnes autorisées

La seconde étape est l'identification des collectivités territoriales et de leurs groupements pouvant acquérir, installer et entretenir un dispositif de vidéoprotection. Sont ainsi listés les communes, les établissements publics de coopération intercommunale, les syndicats mixtes, les conseils départementaux et les conseils régionaux.

Vient ensuite l'identification des agents territoriaux habilités et des élus locaux habilités à procéder au visionnage des images issues des systèmes de vidéoprotection mis en œuvre par les collectivités territoriales et leurs groupements. Les agents de police municipale ont une compétence de principe en la matière. Cette compétence est étendue aux agents territoriaux agréés par le représentant de l'Etat dans le département : cela concerne les agents territoriaux des communes et des EPCI à fiscalité propre qui n'appartiennent pas aux cadres d'emplois de la police municipale, ainsi que les agents des syndicats mixtes de mutualisation. Enfin, en tant qu'autorité de police municipale, officier de police judiciaire et autorité fonctionnelle sur les agents de visionnage, le maire a le pouvoir de visionner les images concernant son territoire.

Deux conventions

Le gouvernement explique ensuite les modalités d'organisation et de financement des dispositifs de vidéoprotection mutualisés. Deux conventions obligatoires sont en effet prévues dans le cadre de la mutualisation des dispositifs de vidéoprotection, que celle-ci soit réalisée au niveau de l'EPCI à fiscalité propre ou d'un syndicat mixte :

- la convention conclue entre la structure de mutualisation et chacun des membres concernés par le dispositif de vidéoprotection mutualisé ;
- la convention conclue entre la structure de mutualisation et les services de l'Etat.

Caméras dites « augmentées » dans les espaces publics : la position de la CNIL

À l'issue d'une consultation publique, la CNIL publie sa position sur les conditions de déploiement des dispositifs de vidéo « augmentée » dans les lieux ouverts au public. Elle y présente notamment le cadre juridique actuellement applicable et souligne les risques pour les droits et libertés des personnes.

Une priorité stratégique pour la CNIL

Depuis 2017, la CNIL appelle à la vigilance concernant les évolutions des outils de vidéoprotection et l'inadéquation du cadre légal avec certaines technologies parfois déployées. Pour autant, depuis plusieurs années, de nouveaux types de caméras équipées de logiciels d'intelligence artificielle se développent. Il s'agit par exemple de dispositifs qui filment la voie publique et peuvent comptabiliser en temps réel les différents usages (piétons, voitures, vélos) afin de les répertorier, ou encore qui comptabilisent et catégorisent (genre, âge, etc.) les personnes fréquentant un centre commercial afin d'adapter les contenus publicitaires ou l'agencement des enseignes ou des produits.

Ces caméras soulèvent de **nouveaux enjeux pour les droits et libertés des personnes**, et de nombreux professionnels ou associations ont interrogé la CNIL sur leur encadrement juridique. La CNIL a souhaité exposer ses réflexions et ses analyses sur le sujet d'un point de vue éthique, technique et juridique.

Elle a ainsi **publié un projet de position qu'elle a soumis à une consultation publique durant deux mois,** pour permettre à l'ensemble des parties prenantes (citoyens, administrés, consommateurs, industriels/fournisseurs de solutions, utilisateurs de solutions, chercheurs, universitaires, associations, etc.) de s'exprimer.

Les contributions reçues par la CNIL, nombreuses et variées, ont permis d'enrichir et de consolider sa position, qu'elle publie aujourd'hui dans sa version finalisée**.**

De quoi parle-t-on ?

La présente position de la CNIL **ne concerne pas les dispositifs de reconnaissance biométrique** et **les usages des dispositifs de vidéo « augmentée »** dans des lieux non ouverts au public (par exemple bureaux, réserves ou entrepôts de magasins...), dans un cadre strictement domestique et en temps différé.

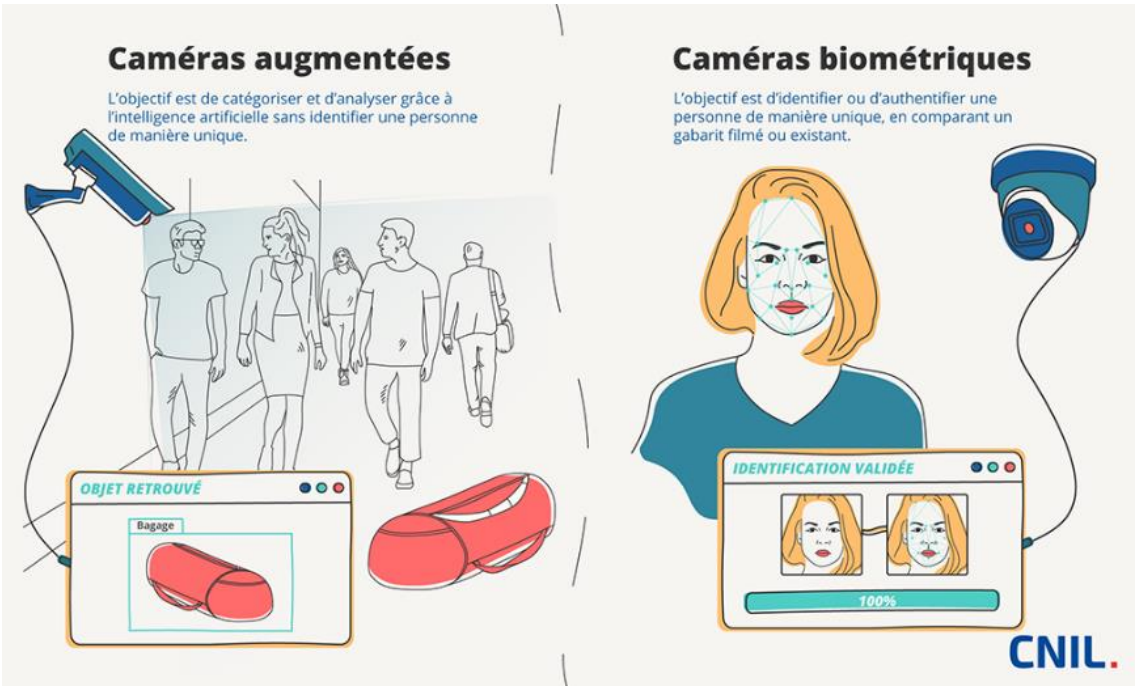
Caméras biométriques et caméras « augmentées » : quelles sont les différences ?

La position de la CNIL concerne les dispositifs de vidéo « augmentée » qui se distinguent des dispositifs de reconnaissance biométriques comme par exemple les dispositifs de reconnaissance faciale. Deux critères permettent de distinguer ces dispositifs :

- la nature des données traitées : caractéristique physique, physiologique ou comportementale ;
- l'objectif du dispositif : identifier ou authentifier de manière unique une personne.

Un dispositif de reconnaissance biométrique cumulera toujours ces deux critères tandis qu'une caméra « augmentée » n'en remplira aucun (par exemple une caméra « augmentée » qui filme la rue pour classer les différents usages : voitures, vélos, etc.) ou seulement un des deux (par exemple une caméra « augmentée » qui détecte les bagarres dans une foule).

Cette distinction a des conséquences juridiques : les dispositifs de reconnaissance biométrique impliquent des traitements de données dites « sensibles » qui sont, par principe, interdits par le RGPD et la loi Informatique et Libertés, sauf exceptions.



Des risques nouveaux pour les droits et libertés individuelles

Une technologie d'analyse automatisée d'images par nature intrusive

La notion de caméra ou vidéo « augmentée » désigne des dispositifs vidéo auxquels sont associés des logiciels permettant une analyse automatique de l'image afin de détecter par exemple des formes ou des objets, d'analyser des mouvements, etc. **Ces caméras sont, par nature, très différentes de celles traditionnellement déployées :** les personnes ne sont plus seulement filmées mais analysées de manière automatisée, en temps réel, afin de collecter certaines informations les concernant.

Ces nouveaux outils vidéo peuvent conduire à un **traitement massif de données personnelles**, potentiellement à l'insu des personnes du fait du caractère « invisible » des logiciels d'analyse d'images associés aux caméras.

Un risque accentué de surveillance généralisée

Le risque d'une surveillance généralisée induit par la multiplication des dispositifs vidéo, pointé depuis longtemps par la CNIL, prend aujourd'hui une nouvelle dimension avec l'essor des dispositifs de vidéo « augmentée » : **cette surveillance se double d'une analyse des personnes**.

Le déploiement de ces dispositifs dans les espaces publics, où s'exercent de nombreuses libertés individuelles (liberté d'aller et venir, d'expression, de réunion, droit de manifester, liberté de culte, etc.), **présente incontestablement des risques pour les droits et libertés fondamentaux des personnes et la préservation de leur anonymat dans l'espace public**.

Ces dispositifs posent également de nouveaux enjeux pour les personnes lorsqu'ils ont vocation à **automatiser entièrement certaines activités de la vie courante**. Des actes simples de la vie quotidienne pourraient ainsi être filmés et analysés par des caméras « augmentées », renforçant encore le sentiment de surveillance des personnes à mesure que ces dispositifs se généraliseront dans les espaces publics : rues, transports, commerces, lieux culturels et sportifs, etc.

Un encadrement juridique spécifique nécessaire

En l'absence de textes spécifiques encadrant l'usage des dispositifs de vidéo « augmentée », **la CNIL a analysé les principes applicables à ces dispositifs par rapport à la réglementation actuellement en vigueur.**

Elle a notamment considéré que le Code de la sécurité intérieure, qui fixe le cadre applicable aux dispositifs de vidéoprotection traditionnels, n'était pas adapté à cette nouvelle technologie. Mais il n'interdit pas non plus son déploiement. La CNIL appelle plus particulièrement l'attention sur trois points.

La nécessité de respecter les grands principes de la réglementation protégeant les données personnelles

Tout acteur qui souhaiterait déployer un dispositif de vidéo « augmentée » devra **se fonder sur une base légale déterminée au cas par cas**. Si aucune n'est exclue ou privilégiée par principe, la **base légale de « l'intérêt légitime »** ne doit pas conduire à un déséquilibre manifeste entre les intérêts poursuivis par l'utilisateur d'un dispositif de vidéo « augmentée » et les attentes raisonnables des personnes (par exemple un magasin qui analyserait l'humeur des clients pour leur afficher des publicités adaptées). De façon plus générale, il faut faire, au préalable, une démonstration **de la proportionnalité** (c'est-à-dire des conditions de mise en œuvre du dispositif par rapport aux objectifs poursuivis) **du dispositif** envisagé.

À ce titre, des mécanismes effectifs de **protection des données et de la vie privée dès la conception (*privacy by design*)** doivent être mis en œuvre pour permettre de réduire les risques pour les personnes concernées. Des **garanties fortes consistent, par exemple, à intégrer des mesures permettant la suppression quasi-immédiate des images sources ou la production d'informations anonymes.**

La nécessité d'une loi pour la mise en œuvre de certains dispositifs

La CNIL rappelle que les dispositifs les plus intrusifs, c'est-à-dire ceux susceptibles de modifier les conditions fondamentales d'exercice des droits et libertés fondamentaux des personnes, ne pourront être déployés que si une loi les autorise et les encadre spécifiquement.

Elle estime notamment que les services de police de l'État ou les collectivités territoriales ne sont pas autorisés par la loi à brancher sur les caméras de vidéoprotection des dispositifs d'analyse automatique permettant de repérer des comportements contraires à l'ordre public ou des infractions.

La question spécifique du droit d'opposition des personnes concernées

Les personnes filmées et analysées par les dispositifs de caméras « augmentées » disposent de droits reconnus par la réglementation sur la protection des données (droit à l'information notamment). Parmi ceux-ci, figure souvent la possibilité de s'opposer au traitement mis en œuvre.

Or, la CNIL a constaté que les personnes ne peuvent généralement pas s'opposer à l'analyse de leurs images, par exemple, lorsque les algorithmes ne conservent pas les images, ou que les conditions d'exercice de ce droit ne sont pas praticables (marquer son opposition impose d'appuyer sur un bouton, de faire un geste particulier devant une caméra, de stationner dans une zone dédiée, etc.).

À ce stade, **la CNIL considère que la mise en œuvre de caméras augmentées conduit fréquemment à limiter les droits des personnes filmées.**

Une telle limitation des droits n'est possible que dans deux cas de figure :

- **soit le traitement impliqué par le dispositif de vidéo « augmentée » poursuit une finalité statistique au sens du RGPD** : c'est-à-dire que le traitement ne tend qu'à la production de résultats statistiques constitués de données agrégées et anonymes. Le traitement n'a pas de vocation directement opérationnelle ;
- **soit le droit d'opposition est écarté, sur le fondement de l'article 23 du RGPD, par un texte spécifique, de nature au moins réglementaire**. Cet acte devra acter la légitimité et la proportionnalité du traitement opéré au regard de l'objectif poursuivi, la nécessité d'exclure la faculté pour les personnes de s'y opposer, tout en fixant des garanties appropriées au bénéfice de ces dernières.

Dans de nombreux cas, il sera donc nécessaire que des textes, réglementaires ou législatifs, autorisent l'usage des caméras augmentées dans l'espace public. Cette analyse juridique rejoint la nécessité politique pour la puissance publique de tracer la ligne, au-delà du « techniquement faisable », entre ce qu'il est souhaitable de faire d'un point de vue éthique et social et ce qui ne l'est pas dans une société démocratique.

Vidéoprotection : La CNIL rappelle le cadre juridique aux collectivités

En mai 2021, la Commission nationale de l'informatique et des libertés (CNIL) mettait en garde la commune de Valenciennes en raison du « *caractère particulièrement intrusif* » du dispositif de traitement de lecture automatisée des plaques d'immatriculation qu'elle envisageait de mettre en place [1].

Plus récemment, d'autres dispositifs « vidéo » ont attiré l'attention de la CNIL, laquelle a déclaré par un communiqué du 23 décembre 2021 avoir cette fois mis en demeure une commune française – dont le nom n'a pas été rendu public – de satisfaire aux exigences de protection des données issues de la loi « Informatique et Libertés » [2] et du code de la sécurité intérieure dans un délai de 4 mois.

Le nécessaire équilibre entre ordre public et libertés individuelles

Si de nombreux dispositifs « vidéo » sont aujourd'hui disponibles et déployés par les collectivités territoriales, la mise en demeure de la CNIL concerne précisément deux systèmes.

En premier lieu, la commune a été sommée quant à la mise en place de son dispositif de vidéoprotection, lequel consiste à filmer la voie publique et tout lieu ouvert au public, à savoir tout « *lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions* » (TGI Paris, 23 oct. 1986, Gaz. Pal. 8 janv. 1987).

En raison de la potentielle atteinte aux droits fondamentaux tels que la liberté d'aller et venir et le droit au respect de la vie privée, la vidéoprotection est strictement encadrée et ne peut être mise en œuvre que pour les motifs énoncés à l'article L.251-2 du code de la sécurité intérieure [3].

Parallèlement, la commune avait équipé les agents de police municipale d'un dispositif de « caméras-piétons ».

Cet usage de caméras mobiles avait été autorisé par la loi du 3 août 2018 relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique et son décret d'application du 27 février 2019.

Au vu du potentiel de ces deux systèmes en faveur de la garantie de l'ordre et de la sécurité publique, permettant notamment de prévenir des atteintes contre les personnes et les biens et de permettre la poursuite des auteurs d'infractions par la collecte de preuves, ils sont aujourd'hui couramment mis en œuvre par les collectivités en complément d'autres systèmes de prévention.

C'est à ce titre que la commune en question avait déployé les deux dispositifs « vidéo » susmentionnés, sans toutefois se conformer aux dispositions applicables en matière de protection des données à caractère personnel à même d'assurer le respect des droits et libertés des personnes.

Cette absence manifeste d'équilibre entre l'ordre public d'une part et les libertés individuelles d'autre part a *de facto* engendré un contrôle, sur place, de la part de la CNIL.

Le processus de mise en place des dispositifs « vidéo » comme garde-fou

La mise en demeure de la CNIL permet de rappeler qu'en raison de leur caractère intrusif à l'instar de « Big Brother », ces dispositifs ne peuvent être librement mis en place par les collectivités.

Bien au contraire, dans un premier temps, dans l'hypothèse où le traitement envisagé serait susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, les collectivités sont avant tout tenues de réaliser une étude d'impact [4] permettant d'évaluer la nécessité et la proportionnalité du dispositif envisagé par rapport aux finalités poursuivies.

Cette étape constitue un préalable nécessaire à la demande d'autorisation auprès de la préfecture territorialement compétente, laquelle, si elle est accordée, permet à la collectivité de procéder à l'installation et à la mise en œuvre du dispositif.

Si la commune mise en demeure par la CNIL avait bien obtenu l'autorisation préfectorale préalable, elle avait omis de répondre aux exigences de l'article 90 de la loi « Informatique et Libertés » tenant à l'analyse d'impact, alors même que le dispositif de vidéoprotection envisagé était bien susceptible de présenter un risque accru pour les droits et libertés des personnes physiques.

Par ailleurs, la commune n'avait notamment pas satisfait à ses obligations d'information découlant de l'article 104 de la même loi, certaines des mentions obligatoires devant figurer sur les panneaux d'affichage ou bien le site de la commune[5] étant manquantes.

La restriction du traitement des images captées par les dispositifs « vidéo » comme garantie

La CNIL vient également souligner tout un corpus de règles applicables à la mise en œuvre des dispositifs « vidéo » litigieux et au traitement des images ainsi captées.

Notamment, outre l'interdiction de visualiser l'intérieur d'immeubles d'habitation, la mise en demeure concerne l'importante question de la durée de conservation des images enregistrées.

Dans son communiqué, la CNIL souligne effectivement l'illicéité des dispositifs déployés par la commune à cet égard.

Pour rappel, l'article L.252-5 du code de la sécurité intérieure prévoit que « *Hormis le cas d'une enquête de flagrant délit, d'une enquête préliminaire ou d'une information judiciaire, les enregistrements sont détruits dans un délai maximum fixé par l'autorisation* » préfectorale, ce délai « *ne [pouvant] excéder un mois.* »

Pourtant, en dépit de ces dispositions, les images issues du système de vidéoprotection relevées dataient de plus d'un mois, celles issues des caméras-piétons ayant quant à elles été conservées plus de six mois, dépassant manifestement la période nécessaire à la prévention et à la détection des infractions pénales prévue par l'article 87 de la loi « Informatique et Libertés ».

Enfin, la CNIL s'avère être très regardante quant à l'accès aux enregistrements vidéo, hors hypothèse du droit d'accès aux images, soulevant dans le cas d'espèce le caractère insuffisamment robuste du mot de passe permettant l'accès au logiciel des caméras-piétons de la commune et l'absence de mesures permettant la traçabilité des accès aux images captées.

Au vu des nombreuses infractions aux dispositions applicables en matière de protection des données, il ne fait pas de doute qu'à défaut de mise en conformité dans le délai imparti, la sanction de la formation restreinte de la CNIL à l'égard de la commune en cas de saisine de la présidente pourrait être sévère.

En définitive, le court délai de 4 mois accordé à la collectivité révèle tout l'intérêt de s'assurer de la conformité de ses traitements en amont de leur mise en œuvre.

Le cabinet **HAAS Avocats**, fort de son expertise depuis plus de 20 ans en matière de nouvelles technologies, accompagne ses clients dans la mise en conformité de leurs traitements à la réglementation « informatique et libertés ». Que ce soit en appui du DPO ou en qualité de DPO externalisé le Cabinet Haas réalise ainsi tout type de mission en lien avec la protection de la vie privée avec deux départements spécialisés sur ces questions : le département Protection des données et le département cyber sécurité.

[1] Enquête Mediapart du 1er août 2021, cf. Vidéosurveillance : Valenciennes et son modèle de « safe city » hor... — Mediapart

[2] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[3] Les finalités légitimant la mise en œuvre de la vidéoprotection tiennent notamment à la protection des bâtiments et installations publics et de leurs abords, à la sauvegarde des installations utiles à la défense nationale, à la régulation des flux de transport, à la constatation des infractions aux règles de la circulation, à la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi qu'à la prévention de fraudes douanières, à la prévention d'actes de terrorisme ou des risques naturels ou technologiques…

[4] Analyse d'impact relative à la protection des données (AIPD)

[5] Le responsable de traitement doit notamment mettre à la disposition des personnes concernées par les dispositifs « vidéo » son identité et ses coordonnées, les coordonnées du délégué à la protection des données, les finalités poursuivies par le traitement auquel les données sont destinées, le droit d'introduire une réclamation auprès de la CNIL et les coordonnées de la commission, l'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée.

DOCUMENT 4

CNIL - 16 mai 2023

Intelligence artificielle : le plan d'action de la CNIL

Devant les récentes actualités sur l'intelligence artificielle, et en particulier des IA dites génératives telles que ChatGPT, la CNIL publie un plan d'action pour un déploiement de systèmes d'IA respectueux de la vie privée des individus.

L'essentiel :

- La CNIL a engagé depuis plusieurs années des travaux pour anticiper et répondre aux enjeux soulevés par l'IA.
- En 2023, elle va prolonger son action sur les caméras augmentées et souhaite élargir ses travaux aux IA génératives aux grands modèles de langage et aux applications dérivées (notamment les chatbots).
- Son plan d'action s'articule autour de 4 volets :
    - appréhender le fonctionnement des systèmes d'IA et leurs impacts pour les personnes ;
    - permettre et encadrer le développement d'IA respectueuses de la vie privée ;
    - fédérer et accompagner les acteurs innovants de l'écosystème IA en France et en Europe ;
    - auditer et contrôler les systèmes d'IA et protéger les personnes.
- Ces travaux permettront également de préparer l'entrée en application du projet de règlement européen IA, actuellement en cours de discussion.

La protection des données personnelles, un enjeu fondamental dans le développement de l'IA

Le développement de l'IA s'accompagne d'enjeux en matière de protection des données et des libertés individuelles auxquels la CNIL s'attache à répondre depuis maintenant plusieurs années. Depuis la publication en 2017 de son rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, la CNIL prononcée à plusieurs reprises sur les questions soulevées par les nouveaux outils amenés par cette nouvelle technologie.

En particulier, **les intelligences artificielles génératives** se développent rapidement depuis plusieurs mois, que ce soit dans le domaine du texte et de la conversation, via les grands modèles de langage (*Large Language Models ou LLMs* en anglais), tels que GPT-3, BLOOM ou Megatron NLG et les agents conversationnels (« chatbots ») dérivés (ChatGPT ou Bard), mais également dans ceux de l'imagerie (Dall-E, Midjourney, Stable Diffusion, etc.) ou encore de la parole (Vall-E).

Ces modèles de fondation (*Foundation models* en anglais) et les briques technologiques qui se reposent sur eux semblent d'ores et déjà trouver de nombreux cas d'application dans des secteurs variés. Néanmoins, la compréhension de leur fonctionnement, de leurs possibilités et de leurs limites, ainsi que les enjeux juridiques, éthiques et techniques autour de leur développement et leur usage restent encore largement en débat.

Considérant que la **protection des données personnelles est un enjeu majeur pour la conception et l'utilisation de ces outils**, la CNIL publie son plan d'action sur l'intelligence artificielle qui vise – entre autres – à encadrer le développement des IA génératives.

Qu'est-ce qu'une IA générative ?

Une intelligence artificielle générative est un système capable de **créer du texte, des images ou d'autres contenus** (musique, vidéo, voix, etc.) **à partir d'une instruction d'un utilisateur humain**. Ces systèmes peuvent produire des nouveaux contenus à partir de données d'entraînement. Leurs performances sont aujourd'hui proches de certaines productions réalisées par des personnes en raison de la grande quantité de données ayant servi pour leur entraînement. Ces systèmes nécessitent toutefois que l'utilisateur spécifie clairement ses requêtes pour obtenir les résultats attendus. Se développe donc un véritable savoir-faire autour de la composition des requêtes de l'utilisateur (*prompt engineering*).

Par exemple, l'image ci-dessous, intitulée « Théâtre d'Opéra Spatial » a été générée par l'utilisateur Jason M. Allen grâce à l'outil Midjourney sur la base d'une instruction textuelle décrivant ses attentes (décor théâtral, toges, inspirations picturales, etc.).

Un plan d'action en quatre volets

La CNIL a engagé depuis plusieurs années des travaux visant à anticiper et à répondre aux défis posés par l'intelligence artificielle, ses différentes déclinaisons (classification, prédiction, génération de contenus, etc.) et ses différents cas d'usage. Son nouveau **service de l'intelligence artificielle sera dédié à ces questions,** et appuiera les autres services de la CNIL qui sont également confrontés à des utilisations de ces algorithmes dans de nombreux contextes.

Face aux enjeux liés à la protection des libertés, à l'accélération de l'IA et à l'actualité liée aux IA génératives, la régulation de l'intelligence artificielle constitue un axe principal de l'action de la CNIL.

Cette régulation se structure autour de **quatre objectifs :**

- Appréhender le fonctionnement des systèmes d'IA et leurs impacts pour les personnes
- Permettre et encadrer le développement d'IA respectueuses des données personnelles
- Fédérer et accompagner les acteurs innovants de l'écosystème IA en France et en Europe
- Auditer et contrôler les systèmes d'IA et protéger les personnes

1. Appréhender le fonctionnement des systèmes d'IA et leurs impacts sur les personnes

Les techniques innovantes utilisées pour la conception et le fonctionnement des outils d'IA posent des questions nouvelles sur la protection des données, en particulier :

- **la loyauté et la transparence** des traitements de données sous-jacents au fonctionnement de ces outils ;
- **la protection des données publiquement accessibles sur le Web** face à l'utilisation du moissonnage, ou *scraping,* de données pour la conception des outils ;
- **la protection des données transmises par les utilisateurs** lorsqu'ils utilisent ces outils, allant de leur collecte (via une interface) à leur éventuelle réutilisation, en passant par leur traitement par les algorithmes d'apprentissage automatique ;
- **les conséquences sur les droits des personnes sur leurs données**, tant en ce qui concerne celles collectées pour l'apprentissage de modèles que celles qui peuvent être fournies par ces systèmes, telles que les contenus créés dans le cas d'IA génératives ;
- **la protection contre les biais et les discriminations** susceptible de survenir ;
- **les enjeux de sécurité inédits** de ces outils.

Ces aspects constitueront un des axes de travail prioritaires pour le service de l'intelligence artificielle et le laboratoire d'innovation numérique de la CNIL (LINC).

Dossier du LINC

Afin de souligner certains de ces enjeux spécifiques aux IA génératives, **le Laboratoire d'innovation numérique de la CNIL (LINC) a publié** un dossier qui leur est consacré**.** Constitué de quatre volets, ce dossier :

- détaille le fonctionnement technique des agents conversationnels récents et rappelle la place centrale des données pour la constitution des modèles de fondation sous-jacents ;
- expose différentes questions juridiques posées par la conception de ces modèles, tant pour la propriété intellectuelle que pour la protection des données ;
- précise les enjeux éthiques des IA génératives pour la fiabilité de l'information, les utilisations malveillantes ainsi que les pistes de la détection et de l'avertissement du public quant à la présence de contenus ainsi générés ;
- illustre par différentes expérimentations les usages positifs ou négatifs qui peuvent être faits de ces outils.

Ce dossier complète les ressources proposées par la CNIL sur son site web pour les professionnels et le grand public.

2. Permettre et encadrer le développement d'IA respectueuses des données personnelles

De nombreux acteurs ont fait part à la CNIL de l'incertitude entourant l'application du RGPD à l'IA, notamment pour l'entraînement des IA génératives.

Afin d'accompagner les acteurs du domaine de l'intelligence artificielle et pour préparer l'entrée en application du règlement européen sur l'IA (en cours de discussion au niveau européen et sur lequel la CNIL et ses homologues européennes avaient publié un avis en 2021), la CNIL propose déjà :

- de premières fiches sur l'IA, publiées en 2022 sur cnil.fr, comprenant notamment des contenus pédagogiques sur les grands principes de l'IA et un guide pour accompagner les professionnels dans leur mise en conformité ;
- une position, également publiée en 2022, sur l'usage de la vidéosurveillance « augmentée » qui utilise l'IA sur des images de l'espace public.

Elle poursuit ses travaux doctrinaux et publiera prochainement plusieurs documents. Ainsi :

- la CNIL soumettra bientôt à une consultation un **guide sur les règles applicables au partage et à la réutilisation de données.** Ces travaux incluront notamment la question de la réutilisation de données librement accessibles sur internet et aujourd'hui utilisées pour l'apprentissage de nombreux modèles d'IA. Ce guide sera donc pertinent pour toute une partie des traitements de données nécessaires à la conception des systèmes d'IA, dont les IA génératives.
- elle poursuivra également ses travaux sur la conception de systèmes d'IA et la constitution de bases de données pour l'apprentissage automatique. **Ceux-ci donneront lieu à plusieurs publications à partir de l'été 2023**, à la suite de la concertation qui a déjà été organisée avec plusieurs acteurs, afin d'apporter des recommandations concrètes, notamment en ce qui concerne la conception des systèmes d'IA comme ChatGPT. Les thématiques suivantes seront progressivement abordées :
    - l'utilisation du régime de la recherche scientifique pour la constitution et la réutilisation des bases de données d'entraînement ;
    - l'application du principe de finalité aux IA à usage général et aux modèles de fondation que sont par exemple les grands modèles de langage ;
    - l'explicitation du partage des responsabilités entre les entités qui constituent les bases de données, celles qui élaborent des modèles à partir de ces données et celles qui utilisent ces modèles ;
    - les règles et bonnes pratiques applicables à la sélection des données pour l'entraînement, au regard des principe d'exactitude et de minimisation des données ;
    - la gestion des droits des personnes et notamment les droits d'accès, de rectification et d'opposition ;
    - les règles applicables concernant la durée de conservation, notamment pour les bases d'entraînement et les modèles les plus complexes à constituer ;
- enfin, consciente que les problématiques soulevées par les systèmes d'intelligence artificielle ne s'arrêtent pas à leur conception, **la CNIL poursuit également ses réflexions éthiques** sur l'utilisation et le partage des modèles d'apprentissage automatique, la prévention et la correction des biais et discriminations, ou encore sur la certification des systèmes d'IA.

3. Fédérer et accompagner les acteurs innovants de l'écosystème IA en France et en Europe

La régulation de l'IA de la CNIL vise à faire émerger, promouvoir et aider à prospérer des acteurs dans un cadre fidèle aux valeurs de protection de droits et libertés fondamentaux françaises et européennes. Cet accompagnement, déjà engagé, prend trois formes :

- la CNIL a lancé depuis 2 ans **un « bac à sable »** pour accompagner les projets et acteurs innovants, ce qui l'a notamment conduite à se pencher sur des projets reposant sur l'IA. Les « bacs à sable » sur la santé en 2021 (12 projets accompagnés) et sur l'éducation en 2022 (10 projets accompagnés) ont ainsi permis de fournir des conseils adaptés à des acteurs innovants de l'IA dans ces domaines. La CNIL ouvrira bientôt

un nouvel appel à projet pour l'édition de 2023, qui concernera notamment l'usage de l'intelligence artificielle dans le secteur public ;
- elle a lancé un programme d'accompagnement spécifique des fournisseurs de vidéosurveillance « augmentée » dans le cadre de l'expérimentation prévue par la **loi relative aux Jeux olympiques et paralympiques de 2024** ;
- enfin, la CNIL a ouvert en 2023 un nouveau programme « d'accompagnement renforcé » pour assister des entreprises innovantes dans leur conformité au RGPD : les premiers lauréats de cet accompagnement renforcé sont des entreprises innovantes dans le domaine de l'IA.

Plus généralement, la CNIL souhaite engager un dialogue nourri avec les équipes de recherche, centres de R&D et entreprises françaises développant, ou souhaitant développer, des systèmes d'IA dans une logique de conformité aux règles de protection des données personnelles.

Ces équipes et entreprises peuvent prendre contact avec la CNIL à l'adresse ia@cnil.fr.

4. Auditer et contrôler les systèmes d'IA et protéger les personnes

La définition du cadre permettant le développement des systèmes d'intelligence artificielle dans le respect des droits et libertés individuelles implique, en aval, que la CNIL en contrôle le respect. Il est donc essentiel pour la CNIL de développer un outillage permettant d'auditer les systèmes d'IA qui lui sont soumis et cela tant de manière à priori qu'à postériori.

L'action de contrôle de la CNIL portera notamment en 2023 sur :

- **le respect de la position sur l'usage de la vidéosurveillance « augmentée »**, publiée en 2022, par les acteurs publics et privés ;
- **l'usage de l'intelligence artificielle pour la lutte contre la fraude**, par exemple pour la lutte contre la fraude à l'assurance sociale, au regard des enjeux liés à l'usage de tels algorithmes ;
- **l'instruction de plaintes déposées auprès de la CNIL.** Si le cadre juridique de l'entraînement et de l'utilisation des IA génératives nécessite d'être clarifié, ce à quoi la CNIL va s'employer, des plaintes ont d'ores et déjà été déposées. La CNIL a, en particulier, reçu plusieurs plaintes à l'encontre de la société OpenAI qui gère le service ChatGPT, et a ouvert une procédure de contrôle. En parallèle, un groupe de travail dédié a été créé au sein du Comité européen de la protection des données ou CEPD (en anglais), en vue d'assurer une démarche coordonnée des autorités européennes et une analyse harmonisée des traitements de données mis en œuvre par l'outil d'OpenAI.

La CNIL sera particulièrement attentive à ce que les acteurs traitant des données personnelles afin de développer, d'entraîner ou d'utiliser des systèmes d'intelligence artificielle aient :

- réalisé une analyse d'impact relative à la protection des données (AIPD) pour documenter les risques et pris des mesures permettant de les diminuer ;
- pris des mesures d'information des personnes ;
- prévu des mesures d'exercice des droits des personnes adaptées à ce contexte particulier.

Grâce à ce travail collectif et essentiel, la CNIL souhaite instaurer **des règles claires, protectrices des données personnelles des citoyens européens afin de contribuer au développement de systèmes d'IA respectueux de la vie privée.**

DOCUMENT 5

La gazette des communes - 31 mars 2022

Comment les industriels de la vidéosurveillance imaginent le futur

Des représentants de firmes spécialisées dans la vidéosurveillance se sont livrés à un exercice de prospective sur le futur de leur secteur.

Encore plus de capteurs, une utilisation encore plus poussée de l'intelligence artificielle, et même des caméras sans objectifs… Réunis par l'Association nationale de la vidéoprotection (AN2V), une structure qui regroupe des entreprises du secteur, des industriels de la vidéosurveillance viennent de plancher, à l'occasion d'une conférence, sur le futur de leur métier à court et moyen terme.

Ainsi, Thomas Wolski, l'un des cadres de la société Bosch security systems, estime que dans un horizon proche les cahiers des charges des appels d'offres vont être étoffés sur le volet de la sécurité des données. "Ce n'est pas encore tout le temps le cas", regrette-t-il, alors que la cybersécurité est une question aigüe pour ces matériels sensibles car très intrusifs.

De même, ce cadre souligne la demande forte des clients finaux pour "avoir plus qu'une image ou une caméra". "L'intelligence artificielle sera encore plus prédictive et mature, signale-t-il de manière générale. Elle deviendra, si elle ne l'est pas déjà, un critère clé dans les cahiers des charges."

Plus d'objets connectés couplés aux caméras

Une autre évolution à court terme anticipée par Laurent Scetbon, l'un des cadres de Hikvision, est celle de la multiplication des objets connectés, qui doivent booster les capacités de surveillance des caméras. Il s'agit par exemple des détecteurs thermiques et des capteurs de chute, qui permettent de faire des décomptes de personne et de repérer des événements anormaux.

Bien évidemment, à un horizon aussi court, les intervenants prêchent d'abord pour leur paroisse. Ainsi, Pascale Demartini, la dirigeante de Sensivic, une entreprise spécialisée dans la détection sonore, plaide pour un développement de ce type de

produits. C'est la réponse, dit-elle, "à la concentration d'informations à analyser dans les centres de supervision urbains".

Mais à plus long terme, à un horizon de cinq ans, la dirigeante espère un "encadrement de l'audioprotection" et la mise en place "d'une réglementation raisonnée". "Il faut un cadre réglementaire clair", soit "un premier terrain de jeu permettant d'exploiter le potentiel des technologies", juge également Nicolas de Cremiers, un cadre de XXII, une société spécialisée dans l'analyse vidéo.

Si les interventions de la plupart des orateurs – en tout, plus d'une dizaine de représentants de sociétés du secteur – sont restées centrées sur les évolutions attendues du marché et des technologies, quelques conférenciers ont ainsi également rappelé l'importance de l'acceptation sociétale de ces futures innovations technologiques.

Dans une prise de position récente sur les dispositifs de caméras "augmentées", la Cnil suggérait la mise en place d'un "cadre juridique clair" permettant "de développer des technologies européennes compétitives incarnant des modèles protégeant la vie privée dès la conception".

Apprentissage automatique

Pour Guillaume Cazenave, le patron de la société de Two-I, spécialisée elle aussi dans l'analyse vidéo, la recherche devrait développer dans les cinq ans des algorithmes d'apprentissage automatique. Une technologie qui permettra, explique-t-il, alors que l'état de l'art est actuellement faible, de "détecter une anomalie sans forcément la décrire formellement", comme un incendie, un regroupement d'une foule ou un accident routier.

Dans le même ordre d'idées, pour faciliter l'exploitation des images produites, Rémy Deutschler, de la société Milestone, anticipe l'arrivée de commandes vocales. "Ce sera intéressant pour les phases de recherche", remarque-t-il. Comme par exemple faire la demande orale d'une recherche, dans les 24 dernières heures, des images comportant une femme avec un pull violet. "Ce sera plus intuitif pour les opérateurs", observe-t-il.

Mais d'autres experts s'attendent également, outre les conséquences de l'arrivée de la 5G et un possible basculement sur « l'informatique en nuage », à davantage d'obligations sur la prise en compte du recyclage sur leurs produits ou encore à une réflexion accrue sur les enjeux éthiques d'une filière pouvant devenir la béquille de régimes autoritaires.

Toutefois, si les différents intervenants étaient invités à se projeter à la décennie suivante, la plupart d'entre eux se sont cantonnés aux évolutions attendues les plus proches. Seul Laurent Scetbon s'est toutefois autorisé un pas de côté en imaginant le futur de la vidéosurveillance à vingt ans. "Il sera alors possible d'avoir des caméras sans objectif", imagine ce cadre de Hikvision. Un scénario de science-fiction déjà possible, de fait, en laboratoire.

Collectivités territoriales : des sénateurs préconisent des mutualisations dans la vidéosurveillance et la cybersécurité

Mutualisation des CSU et des ressources en cybersécurité, valorisation de la fonction de RSSI, utilisation des drones par les polices municipales… Telles sont les recommandations formulées par la délégation sénatoriale aux collectivités territoriales dans un rapport sur les technologies adopté jeudi 20 janvier 2022. « Les maires, pivots de la sécurité dans leur commune, sont au cœur du 'continuum de sécurité' », soulignent les auteurs. « Afin d'accomplir au mieux leurs missions de protection de l'ordre public et de prévention de la délinquance, ils peuvent tirer un grand profit du numérique. »

Cinq ans après un rapport consacré aux « nouvelles technologies au service de la modernisation des territoires », la délégation aux collectivités territoriales du Sénat a souhaité poursuivre sa réflexion sur le sujet et a adopté, jeudi 20 janvier 2022, un nouveau rapport, cette fois dédié à la protection des populations. Une partie est axée sur « la protection de l'ordre public », et l'autre sur la sécurité civile.

L'objectif était double, résume un des auteurs, Antoine Lefèvre (LR, Aisne) : « identifier et analyser les bonnes pratiques locales dans ces deux champs de l'action publique locale, à la fois en milieu rural et dans les zones urbaines », et « formuler des recommandations visant, d'une part, à encourager et sécuriser ces initiatives numériques locales, d'autre part, à supprimer ou limiter d'éventuelles entraves à leur réalisation ».

CSU, DRONES, « VOISINS VIGILANTS »

Le sénateur cite, au titre des bonnes pratiques locales, la mise en place des centres de supervision urbains, estimant qu'ils constituent « une illustration particulièrement intéressante de l'intérêt du numérique pour la protection de l'ordre public ». Sont ainsi mises en avant les démarches de Charleville-Mézières, « ville moyenne investie dans la vidéosurveillance » et du département des Yvelines, qui a créé « un CSU intelligent et interconnecté » auquel les communes du territoire équipées de caméras de surveillance peuvent se relier depuis la loi « sécurité globale » du 25 mai 2021.

Dans leur rapport, Antoine Lefèvre, Anne-Catherine Loisier (UC, Côte-d'Or), Jean-Yves Roux (RDSE, Alpes-de-Haute-Provence) se montrent particulièrement enthousiastes sur le couplage de la vidéosurveillance à l'intelligence artificielle , qu'ils estiment être une « voie prometteuse ». Ainsi, au CSU des Yvelines, les agents « sont la plupart du temps face à des écrans noirs, qui ne s'allument que lorsque les algorithmes détectent une situation anormale dans l'un des lieux surveillés », écrivent-ils.

Autre bonne pratique mise en avant par les élus : l'utilisation de drones par les polices municipales, comme à Istres (Bouches-du-Rhône), « commune pionnière » qui a acquis deux drones au début de l'été 2020. Admettant que ces déploiements ont été faits sur « des bases juridiques fragiles », les sénateurs prévoyaient de suivre « avec vigilance » l'expérimentation de cinq ans introduite dans le projet de loi « relatif à la responsabilité pénale et à la sécurité

intérieure », mais le Conseil constitutionnel a censuré cette mesure dans une décision publiée le même jour que le rapport.

Les rapporteurs plébiscitent en outre le dispositif « Voisins vigilants », qui « paraît présenter un bilan coût/avantages très intéressant ». Près de 700 mairies ont souscrit à l'offre, proposée par l'entreprise du même nom, qui permet de signaler un danger via une application et des SMS. Son président, Thierry Chicha, préconise de l'interconnecter avec le CSU, comme dans la commune de Rognac (Bouches-du-Rhône).

UN « DIRECTEUR STRATÉGIQUE DE LA SÉCURITÉ NUMÉRIQUE »

Si ces innovations « ne sauraient être envisagées comme des expériences à généraliser », les élus formulent des recommandations pour « accentuer » et « sécuriser » la numérisation des collectivités. Ils préconisent avant tout de « recourir aux nouvelles technologies de manière rigoureuse, en réalisant un bilan coût/avantages actualisé et public », indique Anne-Catherine Loisier, en insistant sur la nécessité de « mettre en valeur la plus-value du recours au numérique ». « Il ne saurait y avoir de prévention efficace sans information préalable des populations concernées par les risques majeurs », dispose le rapport.

Dans un contexte de pression de la menace cyber, les auteurs invitent à « sensibiliser les élus et le personnel aux enjeux de cybersécurité », afin d'éviter de créer des « colosses numériques aux pieds d'argile ». Il s'agit aussi de « mettre en place des procédures de continuité et de reprise d'activité » en cas d'incident et de « valoriser » la fonction de RSSI, dont il serait « opportun » de faire « un véritable 'directeur stratégique de la sécurité numérique', en lien direct avec les élus et chargé d'une veille permanente sur la cybersécurité ». Les élus appellent en outre « à veiller à la sécurisation des données ».

RENFORCER LA COOPÉRATION ÉTAT / COLLECTIVITÉS

Ils recommandent par ailleurs de « développer les usages numériques en pleine conformité avec le principe de subsidiarité », autrement dit de « confier la compétence numérique à l'échelon qui assure la meilleure veille technologique, qui dispose des meilleures compétences et qui est le plus efficace en termes de cybersécurité ». Pour eux, il peut s'agir « soit du niveau intercommunal soit départemental ». « Cela permettrait aux petites collectivités, identifiées comme des 'maillons faibles', de bénéficier, par l'effet de la mutualisation, d'une protection numérique renforcée. »

En particulier, les rapporteurs encouragent les élus à « mettre en commun des agents de police municipale dans le cadre des CSU ». « L'objectif est double : d'une part, amortir le coût de réalisation de ces centres, d'autre part, de suivre des images dans une zone géographique aussi étendue que possible. » Mais cette idée se heurte « à la crainte des maires de se voir dépossédés de leur pouvoir de police ». De fait, un « faible » nombre de villes moyennes se lancent dans ces projets, selon l'association Villes de France, qui en évoque deux, dans les communautés d'agglomération d'Ajaccio et de Mont-de-Marsan.

Enfin, le rapport appelle à renforcer la coopération entre les collectivités territoriales et les services déconcentrés de l'État, comme le préconisait déjà la délégation sénatoriale aux collectivités territoriales en janvier 2021. « Ce qu'on souhaite, c'est attiser une vraie culture du numérique sur les territoires », insiste Anne-Catherine Loisier, pour qui le manque de coordination peut se révéler un « frein à ces innovations émergentes ». Pour les sénateurs, la concertation est particulièrement « essentielle » dans le domaine de l'alerte des populations, dans la mesure où le nouveau système d'alerte déployé en juin 2022 nécessitera « une communication efficace et hyper-réactive entre les maires et les services préfectoraux ».

DOCUMENT 7

Nepsio Conseil - 26 avril 2022

Les enjeux de la transition numérique au sein des collectivités

Avec l'évolution massive des usages digitaux dans notre quotidien, la transition numérique est devenue un domaine prioritaire, également au sein des collectivités.

Les services publics font face à de nouveaux enjeux numériques centraux et essentiels, tant de **gouvernance**, **d'organisation** qu'à **l'évolution des besoins des usagers**. Ils se confrontent également à une **réglementation** récente, fixant le cadre et les objectifs numériques pour toutes les collectivités territoriales comme la Loi pour une République numérique du 7 octobre 2016, Loi n° 2016-1321, qui prépare le pays aux enjeux de la transition numérique et de l'économie de demain. Les attentes renforcées des usagers pendant la crise sanitaire ont d'ailleurs incité le gouvernement à mobiliser 1,7 Milliards d'euros pour soutenir la **transformation numérique de l'Etat et des collectivités territoriales** dans le cadre du **plan de relance.** Garantissant **simplicité, rapidité et proximité d'usage**, le numérique et la digitalisation ont le potentiel de devenir de véritables outils renforçant la qualité de la relation entre le service et l'habitant.

Au-delà de cet intérêt évident, ils constituent également une opportunité majeure pour le **maintien de la souveraineté** et de **performance organisationnelle** d'une collectivité. Plus précisément, dans quelle mesure la **maturité numérique** des collectivités relève-t-elle **d'enjeux fondamentaux d'acculturation et de maîtrise de la donnée ?**

Des enjeux de gestion des ressources humaines

Le numérique est non seulement un sujet d'amélioration de la relation aux usagers : c'est aussi un **sujet organisationnel central et de grande ampleur.** Engager la transformation numérique dans une collectivité, c'est engager une transformation en profondeur de l'organisation, en passant tant par une réflexion sur le niveau **d'acculturation au numérique des agents**, que sur ses **méthodes de management** et ses **outils**.

De fait, 60% des agents territoriaux estiment avoir besoin d'être formés au numérique pour améliorer leur autonomie et leur qualité de vie au travail [1]. Ils font face à des transitions **rapides et parfois à marche forcée** qui nécessitent une **compréhension** et une **maîtrise sécurisée et sécurisante** de leur environnement numérique. Une grande majorité des métiers (communication, finances, planification, métiers d'accueil…) est exposée à la **dématérialisation des procédures**. Cela nécessite de fait une montée rapide en compétences. Dans une démarche d'accompagnement RH, tout l'enjeu est donc d'identifier **les besoins et les compétences** les plus pertinentes à mobiliser pour les différents métiers donnés. Ainsi, la capacité d'un service public à adopter de **nouvelles méthodes de travail** (basées par exemple sur l'agilité ou le design thinking) est un déterminant fort de réussite dans ce nouveau contexte.

66% **Des participants n'ont pas le bagage suffisant pour être en maîtrise sur l'ensemble des situations professionnelles pouvant être vécues sur un poste intégrant une dimension numérique (Pix-2021)**

25% **Sont en grande difficulté (Pix-2021)**

Au-delà du développement de nouvelles méthodes de travail, pour une montée effective en compétences, toute démarche de digitalisation des services doit aussi s'accompagner d'une

[1] Enquête : compétences numériques des agents territoriaux- PIX

amélioration des conditions de travail des agents par **l'accès et l'appropriation de nouveaux outils.** On peut notamment penser aux outils interfacés (entre services ou collectivités) permettant en plus d'une simplification administrative, le développement d'un travail en **transversalité**. Cette digitalisation transverse de la collectivité simplifie de surcroît les processus métiers. Le numérique sert ainsi une boucle vertueuse et la **diffusion de la culture d'un « mode projet »,** qui engendre des réflexions importantes sur la manière dont s'organisent les services (par exemple : modification/ réduction du nombre d'échelons hiérarchiques), et la manière dont sont **réparties et mobilisées les compétences** (développement de la transversalité, souplesse et réactivité…).

Cette stratégie s'intègre également dans un **contexte national** (avec par exemple la sélection de logiciels ou de systèmes de gestion des données français plutôt qu'étrangers, ou en évitant le recours aux GAFAM), mais aussi dans un **contexte européen** (choisir des solutions qui interdisent la sortie des données des habitants hors des frontières de l'UE afin de pouvoir pleinement bénéficier de la protection du RGPD.

Qualifiée par certains de « nouvel or noir », la question de la capacité à **maîtriser, protéger puis valoriser** les données territoriales se pose chaque jour pour une **élaboration viable et pertinente des politiques publiques**. C'est ici tout l'art de l'analyse des données pouvant permettre de mieux appréhender les dynamiques des territoires, de mieux cibler et anticiper les besoins des habitants, et, in fine, de mieux mesurer l'impact des politiques locales.

Ces améliorations vont de **l'organisation des matières premières à celle des équipes, en passant par la maintenance des machines**. Il s'agit de chantiers de longue durée, exercés de manière itérative grâce à des outils comme AX2012.

En effet, il est très important dans ce type de projet de prendre le temps de faire les choses avec habileté et prudence, car les employés doivent s'adapter aux nouveaux moyens de fonctionnement petit à petit, afin que cela fasse partie intégrante de leur travail.

Des enjeux de la maitrise de la donnée et de la souveraineté

Si elle représente une opportunité notable pour la **performance organisationnelle** des collectivités territoriales, la transition numérique représente aussi des enjeux certains en matière de **souveraineté et de maîtrise de la donnée** à plus large échelle.

La souveraineté numérique désigne la capacité à *"maîtriser l'ensemble des technologies, tant d'un point de vue économique que social et politique",* et de "*se déterminer pour avoir sa propre trajectoire technologique*" (Bernard Benhamou). Open data, big data, data center… Les collectivités font face à ces variations puissantes qui redessinent les champs d'actions, les manières de faire et les attentes des usagers. Le sujet de la maîtrise des données est un enjeu existentiel, en tant que le pouvoir d'action sur le territoire passe par une gestion réussie des données (dont le meilleur exemple reste celui de la Smart City). Du pilotage stratégique du territoire aux interventions des services techniques, la capacité à accéder et valoriser les données devient un enjeu de souveraineté pour les collectivités.

Cet enjeu repose sur **le choix d'outils** qui garantissent au service public qu'il conserve la **maîtrise** à travers le **contrôle de ses propres données et de celles générées par les acteurs** qui parcourent son territoire (usagers, prestataires…). Via le respect des règles RGPD par exemple, elle doit s'assurer que les prestataires (hébergeurs, délégataires de service public…) ne s'approprient ni ne diffusent les données publiques. La souveraineté doit alors permettre à la collectivité de discuter d'égal à égal avec l'ensemble des acteurs du territoire.

Le numérique : un enjeux fondamental pour les collectivités

Le **numérique** s'inscrit comme un **outil clé dans le développement d'une collectivité et de ses services internes.** De surcroît, force est de constater qu'il sert aussi des enjeux **d'accessibilité, d'efficacité et de proximité** pour l'usager, mais aussi **d'attractivité et d'image** des territoires (une transition numérique réussie permettant de faire rayonner auprès des usagers l'image d'une administration modernes, en maîtrise des outils numériques du XXIème siècle.). Pour finir, relever les enjeux de transition numérique au sein d'une collectivité, c'est aussi résolument lutter contre **l'illectronisme numérique** qui touche près de 17% de la population (INSEE). **La lutte contre la fracture numérique (avec les moyens humains, techniques, financiers correspondants)** représente alors un **facteur de succès de la stratégie numérique**.

DOCUMENT 8

Caissedesdepots.fr - 24 janvier 2022

Dans les collectivités, la transition numérique repose aussi sur la maîtrise de compétences numériques

Les évolutions de l'action publique, les attentes fortes des usagers (dématérialisation, accueil et accompagnement du public en présentiel et à distance, open data etc.) renforcées pendant la crise sanitaire, ont incité l'Etat à mobiliser 1,7 milliards d'euros pour soutenir la transformation numérique de l'Etat et des collectivités territoriales dans le cadre du plan de relance.

L'enjeu des compétences numériques des agents territoriaux a été mesuré : 25% d'entre eux n'ont pas une pratique autonome des compétences numériques basiques, telles que l'usage de courriels, d'outils collaboratifs, des fonctionnalités basiques de gestion des fichiers, tandis que leurs métiers évoluent par nature vers davantage de médiation, d'accompagnement des usagers, et l'utilisation d'outils numériques et utilisant des données.

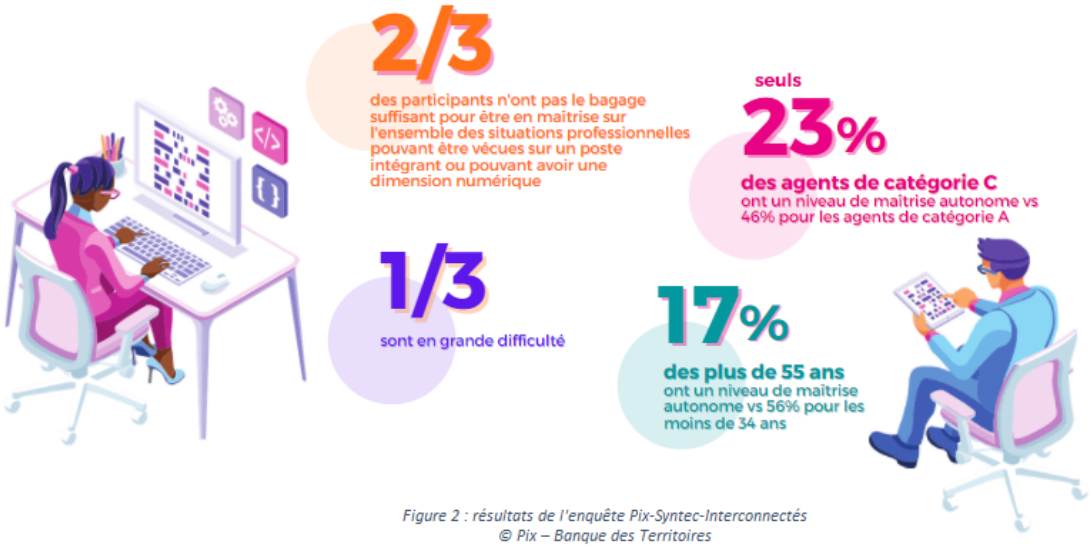


Figure 2 : résultats de l'enquête Pix-Syntec-Interconnectés
© Pix – Banque des Territoires

Ces constats révèlent une marge de progrès encore importante, mais dans les communes, les conseils départementaux et régionaux, les initiatives dédiées à l'autonomie numérique des agents (évaluation, formation, médiation) sont en plein essor.

L'impact du numérique sur les métiers des agents, une préoccupation récente pour les collectivités et qui s'accélère avec le développement du télétravail et de la dématérialisation.

Si l'informatisation du secteur public local a commencé il y plus de 20 ans, la prise de conscience de son impact sur les compétences à maîtriser est beaucoup plus récente.

Le CNFPT a mené une étude relative à l'impact du numérique sur les métiers de la fonction publique territoriale sur plus d'un an auprès de 300 acteurs dont 159 collectivités. Les travaux ont mis en évidence un besoin urgent de développer l'acquisition de compétences socles liées aux usages du numérique.

Toutefois, la numérisation des métiers des collectivités implique également des montées en compétences plus spécifiques. 42 métiers vont nécessiter à court terme une montée en compétences : communication, finances, planification mais aussi les métiers d'accueil et de médiation (services sociaux, voirie, culture, agents d'accueil…) sont particulièrement exposés à la dématérialisation des outils et des procédures.

Pour le CNFPT, les collectivités sont entrées dans "une nouvelle phase de la transition numérique" liés :

- à l'intégration des nouvelles technologies,
- aux obligations réglementaires de dématérialisation, open data…,
- au niveau des pratiques numériques des habitants,
- aux nouveaux modes d'organisation et de travail induits ou favorisés par le numérique comme le télétravail, recours au distanciel, travail en réseau et en mode collaboratif.

L'ensemble des 241 métiers territoriaux sont impactés "dès maintenant" par la transition numérique selon leur analyse.

Passer d'une logique « outil » à une logique « compétences » dans les démarches d'accompagnement

La logique de formations bureautique, outil par outil, a montré ses limites face à la diversité d'outils à manipuler et leur constante évolution. L'approche alternative consiste à cibler l'acquisition compétences permettant d'être autonome dans des situations quotidiennes ou nouvelles, de manière à pouvoir s'adapter aux changements ou à l'arrivée de nouveaux outils, et chercher des réponses par soi-même.

L'Union Européenne a développé un cadre de référence de compétences numériques regroupées dans 5 grands domaines. Ce cadre de référence est un point de départ. Chaque catégorie se décline ensuite en compétences simples (saisir du texte dans un logiciel d'édition) jusqu'à des compétences plus complexes (coder une page web en html).

Dans une démarche d'accompagnement, tout l'enjeu est donc d'identifier celles qui sont pertinentes pour un métier donné, et le niveau de maîtrise attendu.

Un socle de compétences numériques commun à tous les agents, et des compétences spécifiques complémentaires selon les métiers

La Banque des Territoires et son partenaire Pix ont mené des travaux pour identifier les compétences les plus importantes pour les métiers de la fonction publique territoriale. Pix est une startup d'Etat qui s'appuie sur le cadre de référence européen pour proposer un service en ligne permettant de mesurer, développer et certifier ses compétences numériques aujourd'hui utilisé par plus de 7 millions d'utilisateurs.

A ce jour, plusieurs dizaines de collectivité ont déjà mis en œuvre des stratégies d'accompagnement pour :

- Cartographier les compétences numériques maîtrisées ;
- Mettre en place d'un plan de formation adapté aux besoins des agents ;
- Suivre dans la durée de l'acquisition des compétences.

Ces retours d'expériences ont fait apparaître l'intérêt de construire un référentiel de compétences dédié aux collectivités territoriales. Les travaux de la Banque des Territoires et Pix ont permis d'identifier deux groupes de compétences :

- un socle de compétences pour l'ensemble des agents (figure 2)
- et des référentiels orientés métiers (figure 3).

Figure 2 : socle de compétences numériques à maîtriser par tous les agents
© Pix – Banque des Territoires

Figure 2 : socle de compétences numériques à maîtriser par tous les agents
© Pix – Banque des Territoires

Des parcours d'évaluation de ces compétences ont été conçus dans le cadre du partenariat de la Banque des Territoires et Pix. Ils seront expérimentés par une trentaine de collectivités de février à avril 2022. Suite à l'expérimentation, ces parcours seront intégrés à l'offre de Pix dédiée aux collectivités.

Conclusion : Vers une approche intégrée de la transition numérique

L'évolution vers la numérisation de plus en plus de procédures, de services aux usagers et des outils métiers est inéluctable et rend la prise en compte des compétences numériques incontournables.

Toutefois, toute démarche d'accompagnement des compétences doit également tenir compte de l'environnement numérique dans laquelle elle se situe :

- **La connectivité du territoire**, notamment dans les zones rurales et en Outre-Mer, pour lesquels la Banque des Territoires est engagée à offrir des solutions de financement aux collectivités et acteurs privés.
- **La disponibilité des données à jour et de services performants** : du pilotage stratégique du territoires aux interventions des services techniques, la capacité à accéder à des données à jour et à des outils permettant de les exploiter devient un enjeu de souveraineté pour les collectivités.
- **L'accès à du matériel adapté** : avec la numérisation des activités professionnelles, le besoin de matériel adapté (webcam, micro, tablette, smartphone,…) est exprimé par les agents et particulièrement pour les professionnels de la médiation numérique.

Le défi de la digitalisation des collectivités territoriales

Restez informé

Comme pour les entreprises, les mairies, les administrations et les collectivités territoriales traversent une période de transition dont l'enjeu central est la transformation digitale. D'ailleurs, 65 % des intercommunalités souhaitent mieux s'équiper pour accompagner la transformation numérique de leurs services. Bien que le gouvernement ait débloqué des aides, répondre aux nouvelles attentes des citoyens n'est pas si simple. On fait le point.

Les actions menées au niveau national

Lancé le 13 octobre 2017 par le gouvernement, le **programme Action Publique 2022** a mis en place trois principaux axes de travail.

1. La modernisation de l'environnement de travail des agents publics.
2. La baisse des dépenses publiques pour les contribuables, avec un objectif de moins 3 points de PIB d'ici 2022.
3. L'amélioration de la qualité des services pour les usagers : les démarches administratives doivent être plus accessibles, notamment à travers les outils numériques. L'objectif est de dématérialiser tous les services publics d'ici 2022.

Pour atteindre ces objectifs et accompagner les mairies, les administrations et les collectivités territoriales dans la **transformation digitale**, le gouvernement a débloqué un budget de 700 millions d'euros. Qu'en est-il cinq ans après le lancement du programme Action Public 2022 ?

Cinq ans plus tard : le bilan

Depuis 2017, la **transformation digitale des services publics** a bien avancé. Aujourd'hui, les usagers peuvent :

- réaliser leurs démarches fiscales en ligne ;
- bénéficier du prélèvement à la source ;
- recevoir une carte d'identité nationale électronique et numérique suite à une demande de renouvellement (lancé en 2022).

Le plan France Relance dédié aux collectivités

Pendant la crise du Covid, les services publics ont été moins accessibles aux citoyens. Pour ***« stimuler l'innovation numérique et accélérer la transformation numérique des collectivités territoriales et de l'État »***, le gouvernement a introduit le plan France Relance. Les fonds débloqués sont également portés par le programme Transformation numérique des territoires (TNT).

La digitalisation des collectivités et des communes

L'**ADGCF**, ou l'Association des Directeurs Généraux de France, regroupe près d'un millier de cadres dirigeants de communautés de communes, de communautés d'agglomérations, de communautés urbaines et de métropoles. L'association publie en juillet 2018 une grande étude intitulée « L**a transformation digitale des territoires : enjeux et priorités** ».

Les résultats de l'étude : besoins, actions et freins

Voici les résultats qui ressortent de l'étude :

- la digitalisation des services publics est nécessaire pour répondre aux **nouvelles attentes des citoyens**, qui sont de plus en plus connectés ;
- le gouvernement a mis en place des actions (plan France numérique…) pour aider les mairies, les administrations et les collectivités territoriales à digitaliser leurs équipements et leurs services ;
- les bénéfices vont au-delà de l'accessibilité : réduction de l'impact environnemental, dynamisation du territoire, accroissement de l'économie…

Cependant, l'ADGCF a aussi remarqué **trois freins principaux** à la digitalisation des collectivités et des communes :

- 87 % des répondants disent ne pas avoir une vision stratégique suffisamment claire pour avancer ;
- 62 % déclarent ne pas avoir le budget requis pour lancer la transformation numérique ;
- 46 % des répondants indiquent que la digitalisation n'est pas la priorité des élus.
-

Mettre en place une équipe dédiée à la digitalisation ?

L'étude met en avant le besoin pour les collectivités de créer une équipe digitale pluridisciplinaire qui se concentre sur les **attentes des citoyens**. Il s'agirait d'une étape essentielle pour structurer une feuille de route.

Où en est-on de la digitalisation des collectivités ?

Les résultats du Baromètre 2022 de la transformation digitale numérique des territoires, toujours mené par l'ADGCF, montrent que la transformation numérique des TPE et des PME et celle des intercommunalités se sont largement accélérées pendant la crise sanitaire.

Les **budgets dédiés au numérique ont augmenté de 14 %** afin de garantir aux usagers l'accessibilité aux services publics lors des périodes de confinement. La digitalisation des démarches administratives a permis de maintenir le lien entre les mairies, les administrations, les collectivités territoriales et leurs usagers.

Mais un nouvel enjeu stratégique a fait surface : la sécurisation des données stockées en ligne.

Les grands enjeux de la digitalisation

À travers les plans mis en place par le gouvernement, les objectifs sont :

- la **modernisation** des équipements et des services des mairies, des administrations et des collectivités territoriales ;
- l'augmentation de la **productivité** des employés grâce aux solutions digitales ;
- la **simplification** des démarches administratives pour les citoyens à l'aide de nouveaux services numériques.

Un autre défi : réduire les délais

Les Français sont **61 %** à vouloir des délais de réponse plus rapides lorsqu'ils effectuent une démarche administrative. Une attente à laquelle les outils numériques peuvent répondre !

Quels leviers digitaux pour les collectivités ?

La prise de rendez-vous en ligne

Les collectivités peuvent mettre en place des outils simples mais qui correspondent aux attentes des citoyens, comme la **prise de rendez-vous en ligne**. Ce levier peut être utilisé pour les démarches de renouvellement de carte d'identité, de passeport ou pour des services de conseil ou d'aide juridique.

Avec la prise de rendez-vous en ligne, les collectivités profitent de deux avantages majeurs :

- les démarches administratives sont facilitées ;
- la productivité des employés est améliorée.

Des outils de visibilité

Pour développer la visibilité locale des points d'accueil et de contact dans une logique de **Presence management**, il faut :

- harmoniser les informations de l'ensemble des établissements de la collectivité sur toutes les plateformes en ligne ;
- optimiser le référencement des fiches de chaque établissement sur le site PagesJaunes, qui est le média en ligne de référence pour les citoyens.

Un exemple avec France Services

Les maisons France Services ont reçu le Prix d'Or « Solidarité & Inclusion » lors des Cas d'Or du Service Public Numérique 2022, en partenariat avec Solocal.

Pourquoi ? L'Agence Nationale de la Cohésion des Territoires (ANCT) a créé près de 2 500 **maisons France Services** sur l'ensemble du territoire pour rendre les outils numériques plus accessibles aux citoyens et aux entreprises dans le besoin. Solocal a accompagné l'ANCT pour référencer chaque maison France Services sur le site PagesJaunes. Le référencement a été élargi à travers un média accessible aux personnes en situation de handicap pour que les pages des maisons France Services soient trouvées par tous.

Les leviers marketing

Les campagnes de **publicités digitales** et les campagnes de **marketing direct** (envoi de SMS ou d'emails) sont un atout pour les collectivités, qui peuvent les utiliser pour communiquer plus facilement avec les citoyens.

Avec la crise sanitaire, les collectivités se sont digitalisées plus rapidement. Les agents territoriaux se sont adaptés aux nouvelles méthodes de travail, qui correspondent à la transition numérique des équipements et des services. Cependant, les freins demeurent inchangés : les intercommunalités font face à un manque de vision stratégique, de budget et d'accompagnement. Pourtant aujourd'hui, il est indispensable pour les collectivités de se digitaliser : 71 % des Français souhaitent une simplification des démarches administratives grâce à un accès aux services publics en ligne.

Mutualisation de la vidéoprotection : une instruction pour veiller à la bonne mise en œuvre de la loi Sécurité globale

Dans une instruction, les ministres de l'Intérieur et de la Cohésion des territoires attirent l'attention des préfets sur la bonne application des dispositions introduites par la loi Sécurité globale relatives aux nouvelles formes de mutualisation des dispositifs de vidéoprotection via un syndicat mixte.

Les ministres de l'Intérieur et de la Cohésion des territoires ont récemment adressé aux préfets une instruction, datée du 4 mars, visant à la bonne application des dispositions de la loi dite Sécurité globale relatives aux nouvelles possibilités offertes aux collectivités et à leurs groupements de mutualiser des dispositifs de vidéoprotection via un syndicat mixte.

Syndicat mixte fermé ou ouvert restreint

L'instruction rappelle que la loi a créé deux nouvelles possibilités de mutualisation de ces dispositifs dans un périmètre plus large que celui de l'EPCI à fiscalité propre d'appartenance :
- dans le cadre d'un syndicat mixte fermé, composé exclusivement de communes et d'EPCI qui exercent la compétence relative aux dispositifs locaux de prévention de la délinquance (DLPD) ;
- dans le cadre d'un syndicat mixte ouvert restreint, composé exclusivement de communes, d'EPCI qui exercent la compétence DLPD et d'un ou de deux conseils départementaux aux territoires limitrophes.

Dans les deux cas, la circulaire rappelle qu'un double accord est nécessaire : celui de l'ensemble des collectivités et EPCI membres pour opérer cette mutualisation, ainsi que celui de chaque commune d'implantation pour l'installation des moyens de vidéoprotection.

Elle souligne en outre que dans le second cas, les fonctions de président de syndicat ne peuvent être occupées que par le maire de l'une des communes membres ou le président de l'un des EPCI à fiscalité propre membres – condition qui avait donné lieu à de vifs débats au Sénat.

Conventions

La structure de mutualisation doit conclure obligatoirement deux conventions :
- la première avec chacun des membres concernés par le dispositif. Elle fixe les modalités de mutualisation du matériel (acquisition, installation, entretien, mise à disposition) et de mise à disposition du personnel chargé du visionnage, et le cas échéant des moyens financiers alloués par les membres (dépenses de personnel, d'investissement et de fonctionnement) ;
- la seconde avec les services de l'État. Elle définit les modalités d'intervention des forces de sécurité nationales au sein du dispositif de mutualisation et arrête une base juridique organisant notamment la transmission des images entre l'EPCI-FP ou le syndicat mixte et la police ou la gendarmerie nationales. Elle doit être élaborée en cohérence avec les conventions de coordination des interventions de la police municipale et des forces de sécurité de l'État.

Agents habilités non policiers municipaux

La circulaire rappelle également que la loi a étendu la possibilité de visionnage des dispositifs de vidéoprotection aux agents territoriaux des communes et des EPCI-FP qui n'appartiennent pas aux cadres d'emplois de la police municipale, ainsi qu'aux agents de syndicats mixtes de mutualisation. Ces agents doivent toutefois avoir été préalablement agréés individuellement par le représentant de l'État dans le département. Un agrément que ce dernier peut retirer ou suspendre après consultation de l'autorité employeur, ou suspendre sans consultation en cas d'urgence.

Pendant l'exécution de leur mission de visionnage, ces agents sont placés sous l'autorité exclusive du maire de la commune dont ils visionnent les images, à une exception : lorsque le dispositif est mutualisé au niveau d'un syndicat mixe ouvert restreint, et pendant le visionnage d'images prises sur le domaine public départemental – relatives aux biens immobiliers du ou des départements, tels que les routes, abords de bâtiments administratifs, collèges… –, ces agents sont alors placés sous l'autorité exclusive du président du conseil départemental.

Il est également rappelé qu'aucune prérogative judiciaire n'est octroyée à ces agents pour constater des infractions par procès-verbal.

Référence : instruction du Gouvernement du 4 mars 2022) relative à la mise en œuvre des dispositions de la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés portant sur l'acquisition, l'installation et l'entretien de dispositifs de vidéoprotection par les collectivités territoriale et leurs groupements, ainsi que sur l'habilitation du personnel territorial procédant au visionnage (NOR : TERB2205640J).

Surveillance vidéo des lieux publics : comment adapter le cadre juridique ?

La mission parlementaire sur les enjeux de l'utilisation d'images de sécurité dans le domaine public afin de lutter contre l'insécurité propose de faire évoluer le cadre juridique. Il s'agit aussi d'anticiper les évolutions liées à l'intelligence artificielle avec les caméras augmentées.

Enregistré le 12 avril 2023 à l'Assemblée nationale, le rapport sur l'utilisation d'images de sécurité dans le domaine public établit 41 recommandations à même d'anticiper les évolutions technologiques et d'améliorer la gouvernance relative à la vidéosurveillance des espaces publics.

Le cadre juridique complexe de la vidéosurveillance

Depuis l'élaboration du premier cadre juridique régissant la captation d'images de sécurité par la loi du 21 janvier 1995, le **recours à la vidéo** s'est **généralisé**. Les technologies ont évolué et l'intérêt croissant des pouvoirs publics locaux et nationaux a nécessité la mise en place de réglementations. Par exemple, l'installation de caméras de surveillance est soumise à une autorisation préfectorale d'une durée de cinq ans et leur orientation ne doit pas permettre de filmer à l'intérieur des bâtiments. Des règles applicables aux caméras piétons portées par les policiers et les gendarmes ont été fixées en 2016. Les caméras aéroportées par des drones font également l'objet d'une législation.

Cette multiplication des règles entraîne une complexification de la législation encadrant le recours à la vidéo. La mission recommande de **simplifier le cadre juridique**, par exemple :

- en harmonisant les temps de conservation des images en fixant une durée maximale de 30 jours quel que soit le vecteur de captation utilisé ;
- en clarifiant les règles de financement de l'acquisition et de l'installation des systèmes de vidéoprotection par les collectivités territoriales.

Quel cadre pour les caméras augmentées ?

Les **caméras augmentées** repèrent des événements ou des moments précis susceptibles de caractériser un danger. Selon la Commission nationale de l'informatique et des libertés (CNIL), leur utilisation pose le risque d'une "*analyse généralisée des personnes*".

Les caméras augmentées pourraient être **autorisées à l'occasion des jeux Olympiques organisés en France en 2024**. Ces dispositifs comportent de nouvelles fonctionnalités telle que la possibilité de détecter des éléments occultant le visage d'une personne au sein d'une foule. L'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques fixe pour la première fois au niveau législatif le cadre expérimental de l'usage des caméras "augmentées" jusqu'au 31 mars 2025.

Le **recours à la reconnaissance faciale** est actuellement relativement limité en France. Le Conseil d'État a validé le recours à l'outil de reconnaissance faciale dans une décision du 26 avril 2022. Deux traitements automatisés sont créés : le traitement des antécédents judiciaires (TAJ) et le **système de passage rapide aux frontières extérieures (Parafe)**.

Afin d'encadrer le développement de ces caméras, la mission recommande de :

- déterminer un cadre d'évaluation précis et standardisé des expérimentations de dispositifs de vidéoprotection "*augmentée*" ;
- développer un dispositif de certification des logiciels de reconnaissance faciale ;
- désigner un référent national de l'intelligence artificielle qui pourrait être la CNIL ;
- cartographier précisément les emplacements des systèmes de vidéoprotection (environ 38 000 caméras de vidéoprotection sont installées sur la voie publique en zone gendarmerie et près de 52 000 en zone police).

Vidéosurveillance IA : un dispositif déployé dans toute la France après les JO ?

La technologie de vidéosurveillance par intelligence artificielle mise en place durant les JO de Paris en 2024 pourrait être étendue à toute la France de façon permanente après l'événement. C'est ce que vient de laisser échapper la Ministre des Sports…

Du 26 juillet au 11 août 2024, **Paris accueillera les Jeux olympiques !** Une aubaine pour les propriétaires qui vont pouvoir louer leurs logements et gagner des milliers d'euros, mais aussi **une grave menace pour la sécurité nationale**.

Afin de sécuriser les stades et leurs environs, la France a décidé de déployer les grands moyens. Pour la première fois, **une vidéosurveillance IA va être mise en place**.

Les flux vidéo des caméras de vidéosurveillance seront **raccordés à des algorithmes** pour traiter et analyser les images en temps réel. Le but ? Détecter les événements à risque pouvant présenter un risque pour permettre aux autorités d'intervenir sur le champ.

Outre les caméras, **des drones pourront aussi être déployés** dans les airs pour surveiller la foule si la situation l'exige. Le dispositif sera donc très complet.

Le gouvernement promet de ne pas utiliser la reconnaissance faciale

Néanmoins, le gouvernement promet de ne pas utiliser la reconnaissance faciale pour identifier les personnes filmées. L'**IA servira seulement à cerner les situations** inhabituelles et les anomalies.

L'objectif est d'**éviter le risque d'une utilisation détournée**. C'est pourquoi le décret fixe une interdiction d'emploi à des fins d'identification des personnes.

L'**article 2 interdit toute mise en œuvre de reconnaissance faciale**, de manipulation des données biométriques ou de croisement avec d'autres données. Les outils ne pourront pas non plus fonder de décision individuelle ou d'acte de poursuite par eux-mêmes.

Quels seront les événements suspects surveillés par l'IA ?

Le texte de loi a été adopté fin mai 2023 par le Parlement et publié au Journal officiel fin août 2023. Ceci permet de **mieux comprendre quel type de situations** les autorités comptent surveiller.

Il s'agit de la **présence d'objets abandonnés ou d'armes**, le non-respect du sens de circulation, le franchissement d'une zone interdite, **la chute d'une personne**, les mouvements de foule et les départs de feu.

Ces différentes catégories d'événements ont été sélectionnées « *en ce qu'ils sont susceptibles de **présenter ou de révéler un risque d'acte de terrorisme** ou d'atteinte grave à la sécurité des personnes* ».

Des restrictions saluées par la CNIL

La **CNIL a salué cette restriction** à huit types d'événements prédéterminés : « *aucun traitement algorithmique ne pourra être conçu, acquis par l'État ou mis en œuvre en phase d'exploitation pour détecter d'autres événements que ceux qui y sont énumérés* ».

De plus, les **IA se contenteront de signaler les scènes suspectes**. Ce sont des agents humains qui seront ensuite chargés de visionner les images pour confirmer le signalement ou lever le doute.

La **police, la gendarmerie, les services d'incendie et de secours**, ou encore les unités de protection de la SNCF et de la RATP pourront également bénéficier de l'analyse de ces images.

Ils **recevront toutefois une formation** sur la protection des données personnelles et sur l'utilisation du système…

Comme l'a suggéré **la ministre des Sports Amélie Oudéa-Castéra** lors d'un entretien accordé à France 3, le dispositif de vidéosurveillance IA pourrait être **déployé dans toute la France après les JO**.

En réalité, **cet événement sportif va servir de test**. Le gouvernement devra remettre un rapport d'évaluation avant le 31 décembre 2024. Son contenu sera déterminé en Conseil d'État et après avis de la CNIL.

Par la suite, **l'expérimentation sera étendue jusqu'au 31 mars 2025**. En fonction des résultats, il est possible que ce dispositif soit mis en place partout dans le pays d'une façon permanente…

Malgré les restrictions sur la reconnaissance faciale et le nombre limité d'événements surveillés, **les défenseurs de la vie privée dénoncent** ce dispositif de vidéosurveillance jugé intrusif et dangereux.

Selon Noémie Levain, chargée d'analyses juridiques et politiques pour La Quadrature du Net, « *derrière cet outil, il y a **une vision politique de l'espace public**, de vouloir contrôler ce qui s'y passe* ».

Comme elle l'explique, « *Un groupe qui se forme, **cela peut être une manifestation comme un groupe d'amis**. Il y a des considérations morales et politiques dans la conception même de ces outils et qui, pour nous, sont dangereuses. Tout outil de surveillance est une source de contrôle et de répression pour la police et pour l'État* ».

Elle pointe aussi du doigt le fonctionnement des algorithmes basés sur le Deep Learning et les réseaux de neurones : « *c'est un certain type d'apprentissage statistique si complexe que **l'humain ne peut pas comprendre toutes les étapes** du raisonnement. Ces algorithmes vont utiliser des données personnelles et biométriques pour identifier les situations sans qu'on puisse exactement savoir lesquelles sont utilisées* ».

En plus de cette opacité, l'IA confère un immense pouvoir aux autorités : « *On donne à la police un énorme pouvoir qu'elle n'avait pas auparavant, **celui d'être omnisciente**, de voir ce qu'elle ne voyait pas jusqu'ici et de décider ce qui est suspect* »…

De même, l'avocate spécialisée dans le droit de la protection des données personnelles Hélène Lebon estime que la **durée de conservation des images fixées à douze mois** est bien trop longue. En temps normal, les images filmées par des caméras sur la voie publique ne peuvent être gardées plus d'un mois. Elle redoute notamment un piratage et une fuite sur le Dark Web.

Et malgré l'interdiction de la reconnaissance faciale, Noémie Levain rappelle que ces caméras en ont la capacité. Il suffira selon elle d'un **nouveau feu vert législatif pour passer à cette prochaine étape**…

La méthode agile expliquée de A à Z pour faire avancer vos projets avec souplesse

Qu’est-ce qu’une méthode agile ?

Cette **méthode de gestion de projet** est de plus en plus utilisée par les entreprises pour le **développement logiciel**, et parfois pour d’autres types de projets.

Si les mots **Scrum, Lean, sprint, méthode Kanban ou product owner** sont des notions aussi floues que des caractères chinois, rassurez-vous : à la fin de l’article, vous saurez qu’est-ce qu’une méthode agile et comment cela fonctionne.

Nous développerons un peu plus la **méthode agile Scrum** qui est la plus populaire, et vous présenterons quelques outils indipensables.

Levez les barrières et passez à l’agile !

L’agilité est une méthodologie et une philosophie qui dépasse de plus en plus la seule sphère de la gestion de projet. Elle se déploie notamment pour optimiser la gestion de portefeuille de projets (PPM), et même la gouvernance d’entreprise.

Qu’est-ce que la gestion de projet agile ?

La **gestion de projet** agile est une approche qui découpe un projet en différents sous-projets indépendants, appelés itérations, qui vont être répétées jusqu’à atteindre le résultat espéré.

Fonctionnement

Le meilleur moyen d’appréhender les besoins des utilisateurs et du client est de permettre à ces derniers de **tester le produit au fur et à mesure**, en situation réelle.

On évite ainsi l’**effet tunnel**, mentionné plus tôt dans cet article, et on réduit le délai entre la formulation d’un besoin et sa concrétisation. Le produit est enrichi au fur et à mesure et sa conformité est vérifiée régulièrement.

Un produit réussi est celui qui correspond le mieux aux besoins des utilisateurs.

Les changements doivent être considérés comme des **opportunités** plutôt que des obstacles. En effet, de nouvelles idées peuvent émerger et apporter des fonctionnalités au produit non planifiées initialement, et ainsi créer **de la valeur**.

La communication claire et régulière reste la clé en rassemblant tous les acteurs, **sans intermédiaire**. L’**interaction est cruciale** au quotidien pour tendre vers un objectif clair orienté « produit ».

L’idée n’est pas d’élaborer un plan parfaitement détaillé du projet avant même son lancement, mais de **tester les pratiques et les techniques efficientes pour un projet unique**. Grâce aux itérations, l’équipe remet régulièrement en cause sa façon de travailler et se fonde sur une approche empirique pour optimiser son efficacité.

Il est ainsi permis de conserver les méthodes « gagnantes » ou de rejeter les moins efficaces, toujours dans l'optique d'**améliorer le processus de réalisation global**. L'expérience venant avec la pratique, on peut lancer plus tôt le projet et perdre moins de temps à le planifier.

Gestion de projet agile vs gestion de projet traditionnelle

L'agile s'oppose à aux méthodologies classiques de gestion de projet de type **cascade** (*waterfall*) comme le cycle en V. Linéaires et prédictives, elles laissent peu de place aux imprévus et aux changements.

À une époque, elles ont provoqué un taux d'échec des projets informatiques particulièrement élevé, dû à **l'effet tunnel.** Le produit étant livré à la fin, on se rendait parfois compte trop tard que le produit ne répond pas (ou plus) totalement aux attentes à cause du **manque de visibilité** et de flexibilité, pouvant engendrer des r**etards de livraison** ou des dépassements de budget.

La **gestion de projet agile répond à ce problème**, car permet non seulement de prendre en compte les besoins initialement exprimés, mais également les changements ou les nouveaux besoins en cours de développement. On s'assure ainsi que le **produit répond toujours aux attentes.**

Le Manifeste Agile

En 2001, 17 professionnels du développement logiciel se réunissent pour **mutualiser et formaliser leurs bonnes pratiques**. Ils rédigent alors le ***Manifeste Agile***, ou *Agile Manifesto* en anglais.

L'objectif de cette bible de l'agilité ? Encourager l'amélioration du développement de logiciels en s'appuyant sur quatre valeurs :

Nous privilégions… ✓	**plutôt que… ✗**
les individus et leurs interactions	les processus et les outils
des logiciels opérationnels	une documentation complète
la collaboration avec les clients	la négociation contractuelle
l'adaptation au changement	le suivi rigide d'un plan

Il en ressort 12 principes que les équipes agiles adoptent dans leurs méthodes de travail :

1. la **satisfaction client**, la grande priorité ;
2. une **ouverture aux demandes et aux changements,** qui donnent de la valeur au projet ;
3. des **livraisons fréquentes** reposant sur des **cycles courts** ;
4. une **coopération étroite**, voire la co-construction, avec les utilisateurs ;
5. un cadre de travail motivant qui favorise l'**autonomie** des parties prenantes ;
6. les **communications en face à face** sont privilégiées, car plus riches et plus efficaces ;
7. des livraisons d'**éléments opérationnels** uniquement
8. un **rythme soutenable et constant** adapté aux acteurs du projet ;
9. une **qualité technique** de l'équipe pour s'adapter en permanence ;
10. de la **simplicité**, en **allant à l'essentiel** et en minimisant tout travail inutile ;
11. une **équipe autonome,** qui s'organise elle-même pour une meilleure performance ;
12. une **adaptation régulière** des méthodes, processus et outils, pour gagner en efficacité.

Exemple concret d'application de la méthode agile

Prenons l'exemple d'un projet qui doit répondre à un besoin précis : se déplacer.

En utilisant une **méthode de gestion de projet classique**, on construit chaque élément d'une voiture l'un à la suite de l'autre : les roues, puis la carrosserie, le moteur, les phares, le volant, etc. Seuls, ces éléments ne permettent pas de remplir le besoin initial qui est de se déplacer, et il faudra attendre qu'ils soient tous construits et assemblés.

Avec une gestion de projet agile, l'idée est de proposer rapidement une première version très minimaliste (produit minimum viable ou MVP) qui réponde au besoin principal, et de l'améliorer au fil des itérations. Comme le montre le schéma ci-dessous, la première version ne ressemble pas à une voiture, mais plutôt à un skateboard.

L'idée ensuite est de **profiter de retours clients rapides** sur cette première version et d'**améliorer le produit à chaque itération** pour arriver au résultat final de la voiture.

Avantages de la méthode agile

La **gestion de projet agile** :

- permet une **grande souplesse** : les imprévus sont mieux gérés et pris en compte, et vous êtes plus **réactifs** ;
- construit des **relations de confiance et de collaboration** entre l'équipe et le client, grâce à la fréquence et la régularité des échanges ;
- offre une **visibilité en temps réel de l'avancement** du projet, grâce à un contrôle qualité constant. Le client peut demander des ajustements tout au long du projet et vous êtes en mesure d'y répondre ;
- donne une **meilleure maîtrise des coûts**. Après chaque étape, l'équipe fait le point sur le budget consommé pour arbitrer : poursuivre, suspendre ou annuler certaines tâches, voire le projet.

Scrum, la plus célèbre des méthodologies agiles

Scrum est la plus utilisée des méthodes agiles. Elle propose un cadre, ou *framework*, qui néanmoins permet une grande adaptabilité, même pour les projets complexes.

Il définit notamment :

- les rôles et leurs responsabilités, comme celui du **Scrum Master** ou de **Product Owner,**
- des règles sur la durée cycles de développement (appelés **sprints)**,
- des réunions régulières et courtes appelées **cérémonies**,
- un **backlog** qui contient toutes les fonctionnalités à développer,
- différentes pratiques et outils agiles comme le planning poker, le tableau Kanban, ou le scrum board.

Toulouse : comment la ville renforce son arsenal de vidéoprotection

La ville de Toulouse est dotée de 454 caméras. Dix nouvelles caméras connectées via le réseau mobile 4G et 5G seront mises en service fin septembre 2021. DDM - DDM-MICHEL VIALA

La ville de Toulouse va installer dix caméras de vidéoprotection 4G et 5G à des points sensibles de la ville. Des installations plus rapides et moins coûteuses que les caméras classiques.

Face aux problèmes d'incivilités et de délinquance, la Ville de Toulouse va diversifier son arsenal de vidéoprotection. Le maillage de 454 caméras fixes, installées depuis 2014 par l'équipe de Jean-Luc Moudenc, va accueillir dix caméras « mobiles ». Le boîtier en lui-même sera le même qu'une caméra fixe, mais c'est la connectique qui va changer. Pour une caméra fixe, il faut tirer la fibre et le réseau électrique, et souvent installer un mât.

Des caméras plus faciles à installer et à déplacer, et trois fois moins chères que les caméras fixes

Les démarches administratives peuvent prendre plusieurs semaines, et les travaux tout autant. Pour les caméras dites « mobiles », les images seront transmises par les réseaux 4G et 5G, directement au PC vidéo de la police municipale. Les installations se feront donc en quelques jours. Aucune connectique lourde ne sera nécessaire. Les caméras pourront être placées sur un mât déjà existant, un équipement public. Et ces caméras pourront aussi être enlevées et

placées dans une autre rue, un autre quartier, en fonction des besoins. Autre différence entre les deux, et pas des moindres : le coût. Une caméra classique coûte en moyenne 30 000 €, contre à peine 10 900 € pour une caméra « légère », prix auquel il faut ajouter l'abonnement annuel au réseau 4G.

Une première implantation connue, dans les quartiers est de Toulouse

Une première implantation de ces caméras est connue. Ce sera place Marius Pinel, dans le quartier Bonhoure-Guilheméry, près du parc Pinel de l'école élémentaire Bonhoure et du cercle laïque Jean-Chaubet. Les riverains et la police municipale y ont constaté des regroupements, voire du deal, occasionnant des troubles de voisinage. L'implantation sera effective fin septembre 2021.
« C'est typiquement un cas dans lequel ce type de caméras peut être utile. La technologie 4G ou 5G existe, elle a fait ses preuves, il n'y a aucune raison de s'en priver », explique Emilion Esnault, adjoint au maire de Toulouse en charge de la Sécurité. « Nous remarquons que désormais, la question des caméras transcende les clivages politiques. Des maires de sensibilité de gauche, notamment celui de Cugnaux qui appartient au même mouvement politique que l'ancien maire de Toulouse (Génération. s), nous ont rejoints sur cette question » a réagi Jean-Luc Moudenc, maire de Toulouse, lors du bilan de sa première année de mandat de maire dans les quartiers, le 8 juillet.

Plus de cent nouvelles caméras fixes et mobiles d'ici 2026

La municipalité ne s'arrêtera pas là, puisqu'elle a prévu d'installer une centaine de caméras nouvelles pendant le mandat. Une trentaine l'ont déjà été en 2020 et 2021. « On a engagé une consultation avec les policiers de terrain, les habitants, les maires de quartier, pour affiner les besoins, conclut Emilion Esnault. Nous sommes en train de prioriser les besoins, et nous continuerons de déployer les caméras dans les mois qui viennent. »

Une commande groupée de caméras avec d'autres villes

La lutte contre la délinquance ne connaît pas de frontières… Pour faire baisser les prix, plusieurs villes de Toulouse Métropole ont rejoint Toulouse, pour commander des caméras de vidéoprotection. Il s'agit des villes de Blagnac, Seilh, Cugnaux, Aucamville, Aussonne, Colomiers, Beauzelle et Cornebarrieu. « Cette convention permettra à la fois de générer des économies d'échelle pour l'acquisition, l'installation et l'entretien des caméras, et d'harmoniser les dispositifs de vidéo protection sur le territoire », note Emilion Esnault, adjoint au maire de Toulouse et élu à la Métropole. La convention, soumise au vote du conseil municipal de Toulouse le 18 juin dernier, désigne la mairie de Toulouse comme coordinatrice du groupement, et prévoit que chaque collectivité passe un marché distinct. « Toulouse joue un rôle moteur, et fait partager son expertise technique dans le cadre de cet achat groupé », ajoute Emilion Esnault, en faisant remarquer que la vidéoprotection fait désormais consensus parmi les villes, et « transcende les sensibilités politiques ».

DOCUMENT 15

Groupe Videocom - 16 mars 2023

COMINFOS: IOT, Vidéoprotection, Edge computing, 5G, si nous en parlions de façon simple…

L'internet des objets (IoT) est une technologie en constante évolution qui connecte les objets physiques à l'internet, permettant ainsi aux objets de communiquer entre eux. Cette technologie est en train de révolutionner le monde en permettant aux entreprises et aux individus d'optimiser leurs activités et de créer des produits et services innovants.

L'avenir de l'IoT est prometteur, car il est prévu que le nombre d'objets connectés continue de croître de façon exponentielle. Selon certaines études de marché, il devrait y avoir plus de 50 milliards d'objets connectés d'ici 2030.

L'IoT permettra également d'améliorer la qualité de services aux individus, en permettant des avancées dans les domaines de la santé, de la sécurité, de l'énergie et de l'environnement. Par exemple, les dispositifs IoT pourraient aider les personnes âgées ou les personnes souffrant de maladies chroniques à rester à domicile et à recevoir des soins de manière plus efficace.

Cependant, il y a également des défis à relever pour que l'IoT atteigne son plein potentiel. Il est important d'assurer la sécurité et la protection des données des utilisateurs, car les objets connectés peuvent collecter des données personnelles sensibles. De plus, l'IoT doit être accessible à tous, y compris aux personnes vivant dans les zones rurales ou les pays en développement.

L'avenir de la vidéoprotection est lui aussi prometteur, car cette technologie est en constante évolution et les nouvelles avancées technologiques permettent de conserver constamment ses performances. Les progrès récents en matière de reconnaissance faciale, de vision nocturne et de traitement vidéo en temps réel ont permis une surveillance plus précise et efficace.

De plus, l'utilisation de l'intelligence artificielle (IA) permet de détecter plus rapidement les situations à risque, de prédire les comportements suspects et d'automatiser les processus de surveillance. Cela peut aider les entités publiques ou privées à améliorer la sécurité, à réduire les coûts et à rendre la surveillance plus efficace.

Cependant, l'avenir de la vidéoprotection doit également prendre en compte les préoccupations concernant la protection des données personnelles et la vie privée. Il est essentiel que les systèmes de vidéoprotection soient conçus pour être adaptés aux réglementations en matière de protection des données et qu'ils respectent la sécurité et la confidentialité de celles-ci.

Enfin, l'avenir de la vidéoprotection devrait également prendre en compte l'utilisation de l'analyse vidéo pour améliorer les services publics, tels que la gestion du trafic, la collecte de déchets, la surveillance de l'environnement et la gestion des risques naturelles. Cela peut aussi aider les collectivités locales à améliorer l'efficacité de leurs services, à réduire les coûts d'exploitation et à améliorer la qualité de vie des citoyens.

En somme, il est important de poursuivre les avancées technologiques tout en respectant la vie privée, en garantissant la sécurité et la confidentialité des données fournies.

Une caméra connectée est un dispositif qui utilise une connexion Internet pour transmettre des images ou des vidéos en temps réel ou enregistrées sur un serveur distant. L'image d'une caméra connectée peut varier en fonction de son type et de son utilisation. Cependant, voici une description générale de l'image que peut fournir une caméra connectée :

- Résolution : La résolution de l'image dépend de la qualité de la caméra. Les caméras de surveillance peuvent généralement capturer des images en résolution standard ou en haute définition (HD), tandis que les caméras professionnelles peuvent capturer des images en ultra-haute définition (4K ou supérieure).
- Angle de vue : L'angle de vue détermine la taille de la zone capturée par la caméra. Les caméras de surveillance peuvent avoir un angle de vue large ou étroit, selon l'objectif utilisé. Les caméras professionnelles peuvent avoir des objectifs interchangeables pour ajuster l'angle de vue.
- Couleur et luminosité : La caméra peut capturer des images en couleur ou en noir et blanc, selon l'environnement et les besoins de l'utilisateur. La luminosité de l'image peut également être ajustée en fonction de la lumière ambiante.
- Compression : Pour transmettre des images en temps réel, les images sélectionnées par la caméra sont souvent compressées pour réduire leur taille et faciliter la transmission sur Internet. La qualité de l'image peut être affectée par la compression.
- Connectivité : La caméra peut se connecter à Internet via une connexion Radio ou Physique, et la qualité de l'image peut varier en fonction de la qualité du réseau employé.

Il est important de noter que l'utilisation des caméras connectées soulève des questions de sécurité et de confidentialité des données, il est donc aussi important de prendre en compte les mesures de sécurité appropriées pour protéger les données transmises.

L'informatique en périphérie (Edge computing) est une technologie de traitement des données qui consiste à les traiter en temps réel près de la source, plutôt que de les envoyer à un data center. Cette technologie permet de gérer les données plus rapidement, avec une latence minimale, ce qui est important pour les applications qui nécessitent des temps de réponse rapides, telles que la vidéo en direct, la réalité augmentée ...

L'informatique en périphérie peut également aider à réduire la quantité de données envoyées dans le cloud, ce qui peut réduire les coûts de transmission de données et améliorer la bande passante.

L'informatique en périphérie est souvent utilisée dans les réseaux de capteurs IoT (Internet des Objets), où les capteurs collectent des données et les envoient à un nœud de calcul en périphérie pour le traitement. Les données sont ensuite envoyées à un data center pour stockage et analyse ultérieures.

Cependant, l'informatique en périphérie peut également présenter des défis, tels que la cybersécurité et la gestion des nœuds de calcul distribués en périphérie. Il est important de mettre en place des mesures de sécurité appropriées pour protéger les données sensibles, ainsi que des processus de gestion efficaces pour gérer les nœuds de calcul distribués.

En somme, l'informatique en périphérie est une technologie de traitement des data qui peut aider à réduire la latence et les coûts de transmission, en permettant un traitement plus rapide à proximité de la source. Cependant, il est important de prendre en compte les défis de cybersécurité et de gestion de la data lors de la mise en place de cette technologie.

La 5G est la dernière génération de technologie de télécommunications mobiles, qui permet des débits de données plus élevés, une connectivité plus rapide et une latence réduite. L'avenir de la 5G est prometteur et ouvre la voie à des applications innovantes dans de nombreux domaines, tels que la santé, l'éducation, l'automobile, la logistique, etc.

Voici quelques-unes des perspectives pour l'avenir de la 5G :

1. Amélioration de l'expérience utilisateur : La 5G offre des débits plus élevés et une connectivité plus rapide, ce qui permettra aux utilisateurs de bénéficier d'une expérience plus fluide.
2. Internet des Objets (IoT) : La 5G permettra de connecter un plus grand nombre d'objets à Internet, tels que les capteurs, les caméras autonomes, les véhicules… ce qui ouvre la voie à de nouvelles applications dans de nombreux domaines.
3. Industrie 4.0 : La 5G va améliorer l'automatisation industrielle, la maintenance prédictive et les communications entre machines. Cette technologie pourrait aider à l'efficacité des opérations industrielles et à réduire les coûts de production.
4. Santé : La 5G va améliorer la télémédecine, permettant aux patients de consulter des médecins à distance et aux professionnels de la santé d'accéder à des données médicales en temps réel. La 5G pourrait également aider à autoriser des dispositifs de surveillance médicale connectés (maintien des personnes âgées à domicile) et à faciliter les interventions chirurgicales à distance.
5. Voitures connectées et autonomes : La 5G permettra de connecter les voitures à Internet, ce qui améliorera la sécurité routière et ouvrira la voie à la conduite autonome.

Il est toutefois important de tenir compte encore une fois des enjeux de sécurité et de confidentialité des données qui peuvent être associées à cette technologie.

Pour conclure, toutes ces technologies sont et seront de plus en plus présentes dans notre quotidien, tel semble être écrit l'avenir. Au delà de la technique, il faut prendre en compte des notions d'éthique, de confidentialité et de cybersécurité dans chaque déploiement.

C'est une multitude de nouveaux métiers qui vont naître du développement de ces nouvelles technologies et des infrastructures numériques qui en découleront.

Directive NIS 2 : ce qui va changer pour les entreprises et l'administration françaises

Les députés européens ont voté le 10 novembre 2022 la directive NIS 2 qui vise à harmoniser et à renforcer la cybersécurité du marché européen.

En France, de nombreuses entreprises et d'administrations seront soumises à cette nouvelle règlementation. Décryptage avec Yves VERHOEVEN, Sous-Directeur Stratégie de l'ANSSI.

1. En 2016, le Parlement et le Conseil de l'UE ont adopté une première série de mesures concernant la cybersécurité du marché européen. En quoi consistait exactement cette directive connue sous le nom de NIS 1 ?

La transformation numérique des sociétés européennes et l'interconnexion des pays membres ont exposés le marché européen à de nouvelles cybermenaces. Il devenait alors urgent de garantir, collectivement, les conditions de sécurité adéquates pour toute l'Union européenne. C'est pourquoi le Parlement européen et le Conseil de l'Union européenne ont adopté, en juillet 2016, la directive « Network and Information Security » (NIS). Transposée au niveau national en 2018, cette directive avait pour objectif d'augmenter le niveau de cybersécurité des acteurs majeurs de dix secteurs d'activité (ce qui représente quelques centaines d'entités en France). Avec ce premier dispositif, ces grands acteurs ont été soumis à l'obligation de déclarer leurs incidents de sécurité à l'ANSSI, et de mettre en œuvre les mesures de sécurité nécessaires pour réduire fortement l'exposition de leurs systèmes les plus critiques aux risques cybers.

2. Qu'est-ce qui va changer avec l'adoption de la directive NIS 2 ?

La directive NIS 2 est extrêmement ambitieuse. Elle s'appuie sur les acquis de la directive NIS 1 pour marquer un réel changement de paradigme, tant à l'échelon national qu'à l'échelon européen. Face à des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, la directive NIS 2 élargit en effet ses objectifs et son périmètre d'applicabilité pour apporter davantage de protection. Cette extension du périmètre prévue par NIS 2 est sans précédent en matière de réglementation cyber.

3. Pourquoi cette directive revêt une telle importance stratégique pour les pays membres de l'Union Européenne ?

Alors que la menace complexe, professionnelle et en constante évolution ne faiblit pas et que les systèmes d'information restent pour partie vulnérables, la directive NIS 2 représente une opportunité unique : sa mise en application va permettre à des milliers d'entités de mieux se protéger. Elle va être l'occasion de mobiliser largement le tissu économique national et le secteur public. Elle amène aussi les Etats membres à renforcer leur coopération en matière de gestion de crise cyber, en donnant notamment un cadre formel au réseau **CyCLONe** qui rassemble l'ANSSI et ses homologues européens.

4. Quand est-ce que la directive NIS 2 entrera en vigueur ?

La directive, publiée le 27 décembre 2022 au Journal Officiel de l'Union Européenne, prévoit un délai de 21 mois pour que chaque Etat membre de l'UE transpose en droit national les différentes exigences réglementaires. NIS 2 rentrera donc en vigueur en France au deuxième semestre 2024, au plus tard. Certaines exigences seront d'application directe et d'autres devraient être soumises à un délai de mise en conformité.

5. Concrètement, qui sera concerné par le nouveau périmètre d'application de NIS 2 ?

A l'échelle nationale, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés. Environ 600 types d'entités différentes seront concernés, parmi eux des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC40.

6. Qu'en est-il des acteurs de la chaine d'approvisionnement, des administrations et des collectivités territoriales ?

Les acteurs de la chaîne d'approvisionnement, dont les acteurs du numérique, seront soumis au dispositif. Ces nombreux acteurs sont en effet de plus en plus ciblés par des cyberattaques qui visent à atteindre, à travers eux, des clients finaux d'importance plus critiques. Ils verront donc également leur niveau de sécurité numérique renforcé. Autre nouveauté, et non des moindres, les administrations centrales des Etats-membres ainsi que certaines collectivités territoriales intègreront également le périmètre de NIS 2.

7. Toutes les nouvelles entités concernées seront-elles soumises aux mêmes obligations ?

NIS 2 apporte une deuxième évolution majeure. L'inclusion d'un mécanisme de proportionnalité, qui distingue deux catégories d'entités régulées en fonction de leur niveau de criticité : les entités essentielles et les entités importantes. L'ANSSI compte s'appuyer sur cette notion pour définir des exigences adaptées et proportionnées aux enjeux de chacune de ces catégories.

8. La directive NIS 2 est-elle également synonyme d'un renforcement du régime de sanction ?

Le troisième élément majeur de la directive concerne effectivement le renforcement de son régime de sanction, qui s'appliquera à toutes les entités assujetties. Le mécanisme prévu, largement comparable à celui du RGPD, pourra selon les infractions, se fonder sur un pourcentage du chiffre d'affaires mondial de l'entité concernée.

9. Est-ce que la méthode de l'ANSSI va changer avec cette nouvelle règlementation ?

En tant qu'autorité nationale en matière de sécurité numérique, l'ANSSI a toujours veillé à mettre en œuvre des programmes d'accompagnement des organisations adaptés à leur profil. Elle met quotidiennement en œuvre des actions de conseil, de partage d'expertise et d'assistance opérationnelle, tout en favorisant le développement de produits de sécurité et de services de confiance. L'attitude de l'ANSSI a toujours été celle d'un régulateur bienveillant vis-à-vis des entités coopératives, en donnant la priorité à l'accompagnement plutôt qu'au contrôle. Avec la directive NIS 2, l'objectif reste inchangé : élever le niveau global de sécurité numérique en France en permettant aux entités concernées de mieux se protéger face à la menace.

10. Quel type d'accompagnement peuvent attendre de l'ANSSI les entités susceptibles d'être concernées par NIS 2 ?

L'ANSSI est d'ores et déjà mobilisée pour préparer la transposition de la directive et a engagé un dialogue avec les associations regroupant toutes les parties prenantes. Elle amorce ainsi une démarche de co-construction avec les futures entités régulées afin de s'assurer de la pertinence et de la soutenabilité des exigences réglementaires : cette démarche permettra d'obtenir un niveau de préparation au risque cyber à la fois ambitieux et réaliste. L'ANSSI est bien consciente que certaines entités découvriront concrètement les enjeux de la cybersécurité. Son accompagnement se matérialisera par une action de sensibilisation et, si nécessaire, la mise à disposition de nouveaux outils.

11. Comment les entités qui sont concernées par NIS 2 peuvent se préparer à sa transposition dans le droit national ?

L'ANSSI conseille à chaque entité de se préparer dès aujourd'hui. Pour les petites et moyennes entreprises qui intègreront le périmètre, le Guide des TPE/PME constitue par exemple une base solide de mesures concrètes et pérennes. Par ailleurs, pour les entités déjà désignées au titre de NIS 1, il n'est pas d'actualité de relâcher l'effort ! D'ici à l'entrée en vigueur de NIS 2, les exigences de NIS 1 demeurent applicables et l'ANSSI continuera à contrôler leur mise en œuvre. En outre, les futures exigences de NIS 2 s'inscriront dans le prolongement naturel des efforts de NIS 1 et tous les travaux d'ores et déjà entrepris par les opérateurs seront valorisés dans NIS 2. L'ANSSI a bien identifié cette nécessaire continuité comme une priorité de la transposition de NIS 2.

12. L'ANSSI va-t-elle communiquer à nouveau sur le sujet ?

L'ANSSI communiquera sur la directive NIS 2 tout au long de la transposition à l'échelle nationale, partageant à l'ensemble du public le fruit de ses travaux. Nous inviterons d'ailleurs toutes les entités susceptibles d'être concernées par la directive à un rendez-vous dédié à NIS 2, dès le premier semestre 2023.

DOCUMENT 17

lemondeinformatique.fr - 11 décembre 2023

l Act : une régulation européenne tout en compromis

Après plusieurs jours de débat, les institutions européennes se sont accordées sur un texte encadrant l'intelligence artificielle. Cette proposition de règlement tente de ménager l'équilibre entre régulation et innovation, tout en imposant des restrictions et des sanctions. L'UE est effectivement la première puissance à encadrer cette technologie, mais les débats ont été particulièrement âpres entre ceux qui souhaitaient une régulation souple pour ne pas brider l'innovation et les partisans d'un corpus de contraintes sur l'usage de l'IA.

Preuve des tensions sur ces orientations, le ministre Jean-Noël Barrot a indiqué dans un message que le texte constituait « une étape dans un chantier qui s'est ouvert il y a quatre ans qui nécessite des discussions supplémentaires ». Comme d'autres pays, il appelait à la mise en place de « discussions techniques » pour améliorer certains points. Thierry Breton, lui a répliqué, que l'IA Act est « résolument pro-business » et qu' « il n'est plus ouvert à la discussion ».

Une régulation basée sur les risques

Mais que contient exactement le règlement sur l'intelligence artificielle ? En premier lieu, il impose des obligations en fonction du niveau de risque des systèmes d'IA. Le texte insiste sur ceux jugés à « haut risque » entraînant des préjudices pour la santé, la sécurité, les droits fondamentaux, la démocratie…Pour ces systèmes, il sera nécessaire de réaliser une analyse d'impact avant la mise sur le marché. Par ailleurs, une obligation de transparence et d'explicabilité des modèles est mise en place.

La question des IA génératives a provoqué le plus de débats. Il est vrai que l'arrivée depuis un an de ChatGPT d'OpenAI a redistribué les cartes et changé la façon d'appréhender la régulation. La France et l'Allemagne étaient plutôt favorables à une auto-régulation pour protéger leurs champions, Mistral AI (qui vient de mener une levée de fonds de 385 M€) et Alep Alpha (soutenu par SAP ou le groupe Schwarz). Mais les parlementaires européens souhaitaient eux plus de contraintes sur les acteurs (majoritairement américains) dominants. Comme souvent dans l'UE, un compromis a été trouvé avec un modulo des obligations en fonction des « risques systémiques » présentés par les modèles d'IA génératives.

Des interdictions et des exceptions

Autre source de tensions, les systèmes d'IA interdits. Les co-législateurs ont arrêté une liste comprenant « les systèmes de catégorisation biométrique utilisant des caractéristiques sensibles (par exemple : opinions politiques, religieuses, philosophiques, orientation sexuelle, race) ». Il y a aussi l'extraction non ciblée d'images faciales sur Internet ou par vidéosurveillance pour créer des bases de données de reconnaissance faciale. Cela fait notamment référence à la société Clearview, plusieurs fois condamnée en Europe pour ses pratiques de scrapping et de reconnaissance faciale. Les autres interdictions concernent : la reconnaissance des émotions sur le lieu de travail et les établissements d'enseignement, la notation sociale basée sur le comportement ou les caractéristiques personnelles, les systèmes manipulant le comportement humain et exploitant les vulnérabilités des personnes.

À l'ensemble de cette liste, il faut ajouter des exceptions notamment pour les forces de l'ordre. La reconnaissance faciale « à distance » (notamment avec caméra ou drone) est par exemple autorisée « sous réserve d'une autorisation judiciaire préalable et pour des listes d'infractions strictement définie ». Elle concernera « la recherche ciblée d'une personne condamnée ou soupçonnée d'avoir commis un crime grave ». Ce texte donnera certainement lieu à des contentieux où la jurisprudence viendra préciser ces exemptions. Autre domaine bénéficiant d'une exemption, les modèles open source non soumis aux contraintes de transparence. Enfin, une structure de contrôle rattachée à la Commission européenne sera chargée de surveiller la bonne application du texte. En cas de manquement, elle pourra infliger des amendes pouvant aller jusqu'à 35 millions, soit 7 % du chiffre d'affaires mondial. Les États membres vont maintenant travailler sur l'adaptation de leur loi nationale à ce règlement qui devrait rentrer en vigueur en 2026.

Sécurité : Protéger le réseau informatique interne

Les précautions élémentaires

- **Limiter les accès Internet** en bloquant les services non nécessaires (VoIP, pair à pair).
- **Gérer les réseaux Wi-Fi.** Ils doivent utiliser un chiffrement à l'état de l'art (WPA3 ou WPA2 en respectant les recommandations de l'ANSSI sur la configuration de ce dernier) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
- **Imposer un VPN pour l'accès à distance** avec, si possible, une authentification forte de l'utilisateur (ex : carte à puce, mot de passe à usage unique (TOTP).
- **S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet.** La télémaintenance doit s'effectuer à travers un VPN.
- **Limiter les flux réseau au strict nécessaire** en filtrant les flux entrants/sortants sur les équipements (ex : pare-feux, serveurs proxy et autres). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

Ce qu'il ne faut pas faire

- Utiliser le protocole Telnet pour la connexion aux équipements actifs du réseau (ex : pare-feux, routeurs, passerelles). Il convient d'utiliser plutôt SSH ou un accès physique direct à l'équipement.
- Mettre à disposition des utilisateurs un accès Internet non filtré.
- Mettre en place un réseau Wi-Fi utilisant un chiffrement WEP.

Pour aller plus loin

- **L'ANSSI a publié** des bonnes pratiques, par exemple la sécurisation des sites web et la configuration de TLS.
- **On peut mettre en place l'identification automatique de matériel** en mettant en place une authentification des matériels (protocole 802.1X) ou, a minima, en utilisant les identifiants des cartes réseau (adresses MAC) afin d'interdire la connexion d'un dispositif non répertorié.
- **Des systèmes de détection d'intrusion** (IDS) **et de prévention d'intrusion** (IPS) peuvent analyser le trafic réseau pour détecter des attaques, voire y

répondre. Informer les utilisateurs de la mise en place de tels systèmes, après information et consultation des instances représentatives du personnel.

- **Le cloisonnement réseau** réduit les impacts en cas de compromission. On peut distinguer un réseau interne sur lequel aucune connexion venant d'Internet n'est autorisée, et un réseau DMZ (DeMilita- rized Zone) accessible depuis Internet, en les séparant par des passerelles (« *gateway* »). À ce sujet, l'ANSSI a publié des recommandations relatives à l'interconnexion d'un système d'information à Internet (desquelles sont inspirées le schéma ci-dessous).

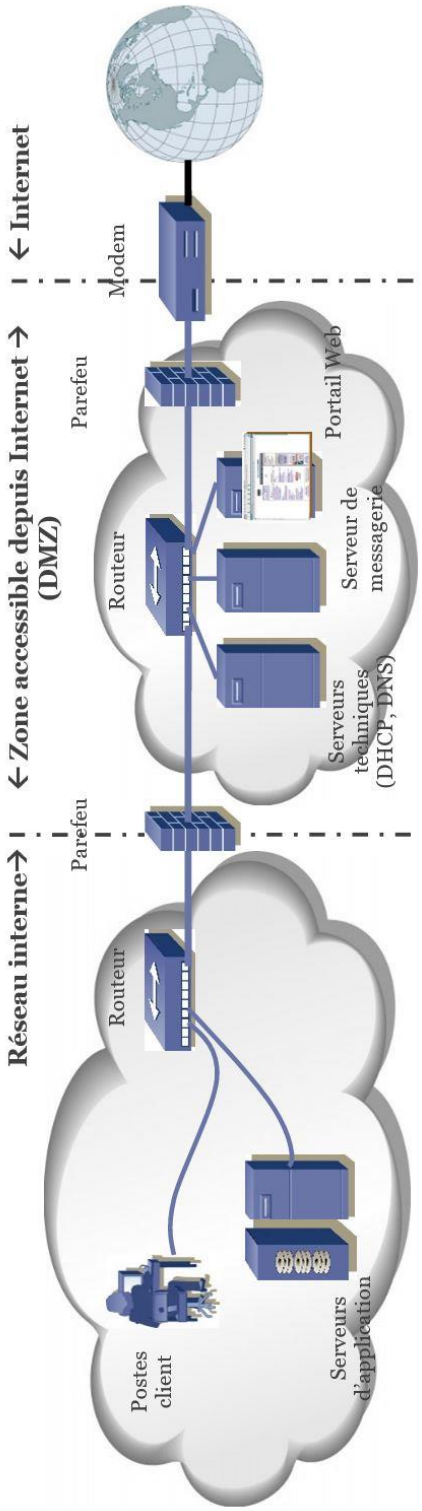


Figure 1: Exemple de mise en œuvre d'une DMZ

ANNEXE A

« Présentation d'INGEAGGLO » - *INGEAGGLO* - 2023

INGEAGGLO est une communauté d'agglomération de 80 000 habitants regroupant 20 communes dont une de 25 000 habitants, 4 de plus de 10 000 habitants et 15 de moins de 5 000 habitants.

INGEAGGLO a mis en place une stratégie en matière de déploiement d'infrastructures haut débit répondant aux objectifs suivants :

- Le déploiement d'ici fin 2024 du "FTTH" (fibre optique jusqu'à l'abonné) sur 12 communes. Ce déploiement est assuré directement par l'opérateur historique Orange sur ses fonds propres. Un partenariat efficace de travail entre INGEAGGLO et la société Orange a été mis en place pour assurer le suivi des travaux.
- Le déploiement, d'ici fin 2024, d'opérations de "montée en débit" (1) (via l'installation d'armoires PRM = Points de Raccordement Mutualisés) sur 3 communes prioritaires de l'espace périurbain de l'agglomération.
- Les 5 autres communes périurbaines ne bénéficient pas encore d'un « bon débit », ce qui nécessite une réflexion sur leurs mises en réseau.

(1) Qu'est-ce que la montée en débit ?

La montée en débit est une technologie intermédiaire qui va permettre très rapidement aux communes isolées qui ne bénéficient pas d'un accès internet correct de bénéficier d'un « bon débit » sur leurs connexions cuivre existantes.
Ceci est rendu possible par la mise en place d'armoire de montée en débit (PRM) raccordée en fibre optique au NRO (Nœud de Raccordement Optique). Ainsi, les débits seront de l'ordre de 25 Mb/s pour un abonné situé à 1200 mètres de l'armoire PRM et jusqu'à plus de 90 Mb/s pour les habitants proches de l'armoire.
Le déploiement de cette technologie passe par plusieurs étapes :
- des travaux de génie civil pour poser la fibre optique ;
- la construction d'une dalle de support pour l'armoire de montée en débit ;
- la pose de l'armoire de montée en débit ;
- la validation par Orange de l'armoire de montée en débit ;
- la mise en service.