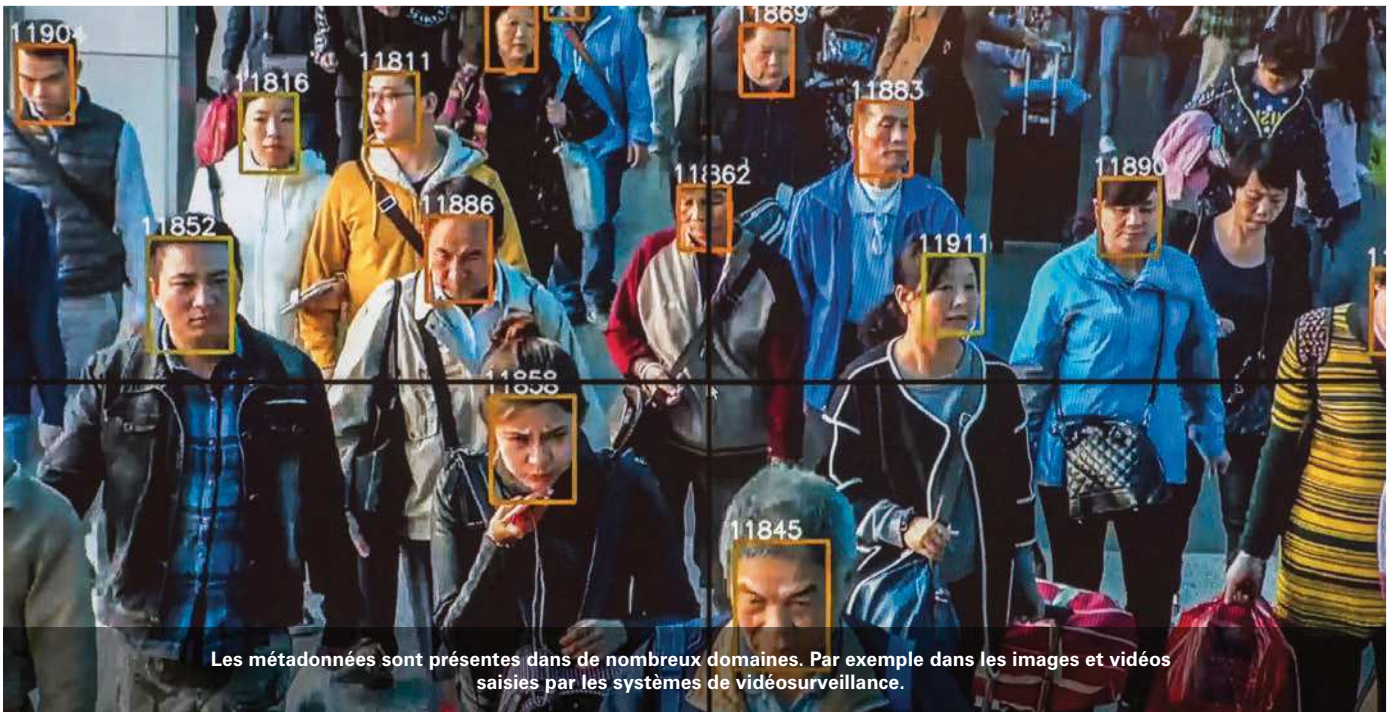

Les métadonnées sont présentes dans de nombreux domaines. Par exemple dans les images et vidéos saisies par les systèmes de vidéosurveillance.

© © Getty image

Des traces partout. Et inexploitées !

Tous les systèmes électroniques enregistrent, constamment, un nombre énorme de données. Par ailleurs, nous laissons des « traces » partout. Et pas toujours en connaissance de cause. Les métadonnées suscitent donc l'intérêt des acteurs de la sécurité. Elles leur ouvrent de nouveaux horizons. Mais pas n'importe comment...

Faisons un peu de pédagogie. Que sont les métadonnées ? *« Une métadonnée est une donnée secondaire, attachée à une donnée principale, qui la complète, la rend intelligible, ou qui la décrit,* explique François Perrachon, Senior VP Global Sales, Public Security chez Idemia. *Si on prend par exemple les photos, il est fréquent qu'y soient associées des données définissant où et quand la photo a été prise, avec quel appareil, quelle ouverture de l'objectif, quel zoom, etc. La photo étant un fichier, il faut, pour la rendre intelligible, un format et une description de la compression d'image qui font également partie des métadonnées. Ce qui est moins fréquent c'est d'avoir des métadonnées qui décrivent le contenu de la photo : un arbre rachitique à gauche, un grand monsieur pressé d'environ 40 ans qui se dirige vers l'arbre, un tableau de Velazquez sur l'affiche de l'abribus… »*

La sécurité elle-même est un vaste domaine dans lequel les métadonnées sont très présentes :

- Dans les images et les vidéos utilisées par la police dans le cadre d'enquêtes. On pourra ainsi savoir, par exemple, à quel endroit une photo a été prise. Et ainsi retracer l'itinéraire d'un suspect grâce aux images.
- Dans les enregistrements audio utilisés par la police dans le cadre d'enquêtes.
- Dans tous les fichiers saisis sur des téléphones portables ou des PC, qu'il s'agisse de fichiers texte, mail, SMS, « cookies » et, bien entendu, les fichiers multimédias. Pour les fichiers, les mails, les SMS, ces données sont exploitées par des moteurs de type mégadonnées qui cherchent à faire des corrélations, des recherches de variations, etc.

Des métadonnées pour quoi faire ? Comment ?

Ces fameuses métadonnées peuvent déjà servir dans le cadre d'enquêtes judiciaires où les métadonnées vidéo et de photo vont permettre, dans un premier temps, de rendre les données saisies intelligibles. La police peut lire une très grande diversité de formats, de compressions, auxquels tous les « non policiers » n'ont pas accès. *« Les métadonnées peuvent aussi permettre de vérifier l'authenticité des données saisies ou, au contraire, être la preuve d'une tentative d'altération*

2 QUESTIONS À

MARIE-CLAUDE FRASSON

Head of Engineering chez Digital Barriers

Le monde de la sécurité – utilisateurs et offreurs de solutions – s'intéresse de plus en plus à l'exploitation possible des métadonnées et à leurs applications dans le cadre de la sécurité. Côté utilisateur, dans quel contexte s'inscrit cette réflexion sur les métadonnées ?

Les pouvoirs publics doivent non seulement protéger les citoyens partout, mais aussi anticiper les menaces en utilisant les données disponibles issues ou non de la vidéosurveillance ainsi que réagir le plus rapidement possible aux alertes générées par les détecteurs en place. Les forces de l'ordre doivent pouvoir effectuer des recherches de preuves et d'indices a posteriori dans les enregistrements de vidéosurveillance le plus rapidement possible. Le défi est énorme. Parallèlement à cela, nous sommes confrontés à une multiplication impressionnante du nombre de caméras et autres capteurs, dont celles portées par les policiers. En même temps, les salles de vidéosurveillance ne sont pas forcément extensibles et un gardien doit surveiller un nombre croissant de caméras à lui seul. À tout cela, s'ajoutent la gestion des fausses alarmes (plus de 10000 alarmes par jour peuvent arriver dans un centre de télésurveillance et seulement 10 % sont pertinentes), la recherche de preuves qui peut mobiliser plusieurs personnes à plein temps, les enquêtes en continu après des dépôts de plaintes (le visionnage d'une heure de vidéo pour rechercher des preuves peut prendre jusqu'à deux heures !), la course au mégapixel par les fabricants de caméras et la saturation des réseaux qui en découle… L'exploitation des métadonnées est une réponse qui semble évidente à ces problématiques car il sera toujours plus facile de faire une recherche sur une base de métadonnées qu'à partir d'une base vidéo. Mais il s'agit d'avoir bien capturé (et stocké !) cette métadonnée lors de l'analyse de la vidéo afin de pouvoir faire des recherches efficaces. Les VMS seront clés dans tout cela mais la route est encore longue. Et malheureusement, il n'existe pas de standard communément utilisé (ONVIF et PSIM n'ayant pas encore été adoptés pour les métadonnées).

Et du côté des technologies ?

Depuis deux ans, les avancées technologiques dans la vidéosurveillance favorisent la réflexion et le recours à l'utilisation des métadonnées. Ainsi, la généralisation des processeurs graphiques (GPU) – autrefois seulement utilisés pour les jeux vidéo et dont les capacités de calcul parallèle sont très bien adaptées aux images – dans les caméras. Ce qui donne des puissances de calcul et d'apprentissage démultipliées. L'arrivée du « deep learning » en intelligence artificielle permet désormais aux ordinateurs d'apprendre de manière non-supervisée à partir d'un ensemble très large de données. Ainsi, après beaucoup d'années très difficiles, nous entrons enfin réellement dans l'ère de l'analyse vidéo car nous sommes confrontés à un problème : il y a trop de données vidéo à traiter et trop peu d'humains pour le faire. Nous n'avons plus le choix : il faut trouver le moyen d'exploiter de manière intelligente cette masse énorme de données. Notre problématique en sécurité s'apparente à celle de la recherche de l'aiguille dans la botte de foin. Si nous pouvons réduire la botte avant de chercher, le temps de recherche sera raccourci. Et les métadonnées peuvent nous aider dans cette tâche. Car nos solutions sont aujourd'hui capables de produire de la métadonnée de plus en plus pertinente, d'améliorer l'indexation du flux vidéo pour faire des recherches plus précises… Par ailleurs, les possibilités offertes par les métadonnées et l'IA peuvent alimenter des applications diverses et variées en plus de la sécurité : marketing intelligent, détection des véhicules restant stationnés trop longtemps aux abords des écoles, calcul automatique des places de parking libres en extérieur... Des applications qui nous paraissaient impossibles il y a encore quelques années sont aujourd'hui à notre portée : compression intelligente qui se base sur l'analyse de l'image pour déterminer quoi compresser le plus (il n'y a, par exemple, pas besoin de détails pour le ciel et le gazon mais pour les visages oui), de l'analyse vidéo très avancée dans la caméra même (comme par exemple dans la détection d'objets en tout genre).

DU CÔTÉ DE LA SÉCURITÉ PRIVÉE

SERVAN LÉPINE

Président d'Excelium

© DR

« L'HOMME AIDERA LA MACHINE À APPRENDRE. »

« L'IA, via l'utilisation des métadonnées, permet beaucoup de choses pour les professionnels de la sécurité. En matière de télésurveillance, par exemple, on peut désormais analyser des flux et détecter des personnes dont la présence sur le site est autorisée, mais dont les droits sont plus ou moins bien encadrés et par toujours bien identifiés, afin de lutter contre les risques internes. On peut aussi développer une analyse plus fine de la réalité des flux à l'intérieur d'un site et en dehors de l'activité des flux classiques. Les données collectées grâce aux systèmes de lutte contre l'intrusion peuvent aussi nous permettre d'apprécier la performance technique et fonctionnelle des systèmes de sécurité. Nous pouvons, grâce aux algorithmes, exploiter des données cycliques, identifier des variations de température, d'hygrométrie, des alarmes techniques, des défauts de liaison téléphonique… Tout cela, sans qu'il soit nécessaire de modifier les paramètres d'une installation. Nous pouvons donc désormais identifier des anomalies et des événements anormaux grâce au big data. Les métadonnées sont aussi une révolution pour le monde de la vidéosurveillance. Mais elles lui posent un défi important : le stockage de ces données dont le volume n'a rien à voir avec celui des données collectées dans l'intrusion. Il n'en reste pas moins vrai que grâce aux algorithmes, à l'IA, aux métadonnées, on sera de plus en plus capables de présenter à un opérateur un événement semblant anormal afin que l'opérateur juge de la justesse de l'information et décide de la manière de la traiter. L'opérateur sera plus actif derrière son écran. Il décidera du bien-fondé d'une alarme. En informera la machine qui apprendra et ne lui présentera plus comme un incident. L'opérateur aidera la machine à apprendre afin, qu'à terme, elle ne lui présente plus que des informations qualifiées et utiles. »

LE POINT DE VUE D'UN PRESTATAIRE

DR. LAURENT GOMEZ
Co-Innovation Lead for Internet of Things chez SAP Products & Innovation


© DR

« LES MÉTADONNÉES SONT UNE FORMIDABLE AIDE À LA DÉCISION POUR L'HUMAIN. »

« Chez SAP, tout ce qui tourne autour du "machine learning" et des métadonnées est un de nos grands axes de travail et de R&D. Nous avons mis au point les briques technologiques qui permettent, sans intervenir sur un réseau de vidéosurveillance et son paramétrage, d'y apporter de l'intelligence et des capacités d'apprentissage. Les métadonnées ne sont pas utiles que pour le secteur de la défense et de la sécurité. On les utilise déjà dans l'agriculture pour détecter des maladies dans des vignobles grâce à des images satellites et des drones. On s'en sert aussi dans le sport pour gérer l'analyse de matchs, les flux de personnes dans les stades, ou dans le domaine du precision retailing. Le milieu urbain est aussi un grand secteur d'utilisation de ce type de données et de l'IA. Cela y permet de gérer les transports, avec les flux de véhicules, le parking ou d'informer les services concernés en cas de crues. Tout l'intérêt du "machine learning" est de se servir des données pour donner la parole aux caméras. Dans les faits, les métadonnées collectées sont corrélées entre elles et analysées afin de fournir en temps réel des informations qualifiées utilisées pour de la levée d'alerte et de l'analyse prédictive. Dans le cadre de notre collaboration avec la Ville d'Antibes, nous distribuons de l'intelligence dans le réseau de 165 caméras afin de détecter les comportements anormaux aux abords d'infrastructures critiques, un comportement suspect aux abords d'une école par exemple… et d'en informer les services de police. Mais toutes les données collectées ne servent pas qu'à des fins sécuritaires. Elles sont aussi très utiles pour gérer des opérations de voirie et, en les corrélant avec celles du trafic urbain, de planifier au mieux les travaux, ou encore pour la gestion de situation de crise en cas de catastrophe naturelle. L'IA fournit alors des métadonnées qui constituent une formidable aide à la décision pour l'humain pour une gestion intelligente et résiliente des infrastructures. Mais ce flot de données représente également un enjeu de cybersécurité majeur. Considérant la nature sensible des données manipulées, SAP œuvre à les protéger des détournements ou de l'utilisation à des fins malveillantes, conformément notamment à la règlementation RGPD. »

● ● ● *de la photo,* ajoute l'expert d'Idemia. *Par exemple, un mécanisme de signature – qui corrèle une métadonnée à la donnée proprement dite par une formule mathématique – peut permettre de vérifier que la donnée proprement dite n'a pas été altérée. Ou faire apparaître des corrélations entre les métadonnées qui peuvent avoir été modifiées de façon incohérente peuvent montrer une volonté de manipulation de l'image (par exemple photo et « imagette » différentes, ou date du GPS et dates de l'appareil photo différentes). »*

Elles ont aussi l'énorme avantage de permettre de comprendre le contexte dans lequel ces données ont été collectées : on peut trouver le lieu, la date, le type d'appareil d'acquisition. Si on a, par exemple, saisi un appareil photo, on pourra identifier tous les lieux où des photos ont été prises par le possesseur de l'appareil, et donc dans quel lieu il s'est rendu. Quand un suspect ne possède pas de téléphone portable, cela peut constituer une source alternative d'information, tout comme l'endroit où il a utilisé sa carte bleue. Quand une grande quantité de photos est saisie, ça permet également d'en faire un classement et une indexation très rapide. Quand un témoin remet une vidéo qu'il a filmée avec son téléphone portable, dans le cadre d'un appel à témoins, il est très facile de vérifier si le témoin propose bien une vue de la scène de crime correspondant prise dans le lieu et à l'heure où s'est déroulé le crime, ou s'il fournit d'autres types d'informations – à condition qu'il n'ait pas manipulé les métadonnées bien entendu. « *Ces données aident, finalement, à comprendre rapidement le contenu des photos,* précise François Perrachon. *En effet, certaines photos contiennent des descriptions, générées automatiquement ou non. Par exemple, sur Facebook, vous pouvez avoir tagué vos amis, et les tags se propagent automatiquement à toutes les photos. Il sera donc très facile de savoir si vous publiez plus de photos montrant Paul ou plus de photos montrant Pierre, et de retrouver toutes les occasions où Pierre et Paul étaient ensemble. »*

Un bouleversement pour la sécurité ?

« L'utilisation des métadonnées dans la sécurité va profondément changer nos métiers, services et autres prestations, reconnaît Servan Lépine, président d'Excelium. *Via les systèmes de sécurité déployés en France – vidéosurveillance, télésurveillance, anti-intrusion, géolocalisation… – nous disposons aujourd'hui d'une masse énorme de données recueillies par tous ces différents systèmes de sécurité électronique. Or, à l'heure actuelle, si on prend uniquement l'exemple de la télésurveillance, seules 5 % des données collectées font l'objet d'un traitement de la part des téléopérateurs d'un centre de télésurveillance. Nous avons donc à notre disposition une masse considérable d'informations qui ne sont pas traitées. »*

Pourtant, l'exploitation de ces données, ne serait-ce que dans la télésurveillance, pourrait permettre d'améliorer grandement les prestations et services proposées par les télésurveilleurs. *« Cela nous permettrait d'aller au-delà de la simple prestation de télésécurité et de proposer de nouveaux services comme le contrôle de l'ouverture et fermeture d'un site, la gestion de la mise en service ou hors service, de tracer les personnes présentes sur site et de les identifier. En fait, d'utiliser de manière optimale les capacités des capteurs déployés sur le terrain à nous fournir de l'information »*, ajoute le dirigeant d'Excelium.

Chez Idemia, les métadonnées sont également perçues comme des ressources à exploiter. De nouvelles formes de traces qu'il faut savoir utiliser. *« Les métadonnées sont générées et enregistrées à l'insu des individus, qui provoquent leur création indirectement. Ce sont de nouvelles traces, comme l'ADN, les empreintes ou les images de vidéosurveillance. En utilisant votre téléphone, votre carte de crédit, votre appareil photo, votre pass Navigo, votre puce de passage rapide au péage des autoroutes, vous générez désormais automatiquement des "traces électroniques" partout sur votre passage »,* explique le Senior VP Global Sales, Public Security de chez Idemia.

Cela n'est pas nouveau ou bouleversant mais il est difficile aujourd'hui de ne pas laisser de « traces ». *« On peut décider de ne pas semer de traces. De même que vous pouvez mettre des gants et des chaussettes pour éviter de laisser des traces papillaires, vous pouvez vous priver de toutes ces nouveautés technologiques qui laissent des traces partout : payez donc vos tickets de métro à l'unité, utilisez votre vieil appareil photo argentique "vintage", ne payez les autoroutes qu'en liquide, ne téléphonez que de chez vous… mais cela est difficile. Et donc, pour la police, qui dit nouvelles traces dit nouveaux leviers pour la résolution de crimes. C'est exactement ce qu'évoquait un ancien chef du service régional d'identité judiciaire de Paris, dans une interview récente réalisée par* Le Monde : *les traces numériques ne sont pas si récentes que ça, mais leurs sources sont de plus en plus nombreuses et surtout la population est de moins en moins capable d'envisager de vivre sans ses compagnons numériques – et donc génère de plus en plus de traces »,* reconnaît François Perrachon.

Des limites tout de même…

Face à cette explosion des métadonnées et la généralisation de leur exploitation, se pose tout de même la question des limites à tout cela. Elles sont évidemment d'ordre technique et juridique. *« Outre les contraintes réglementaires, il faut comprendre que trop de métadonnées tuent la métadonnée,* tient à préciser Marie-Claude Frasson, Head of Engineering Digital Barriers. *Par ailleurs, tout cela suppose qu'il va falloir savoir les stocker, les organiser, faire des recherches. On est qu'au début en termes de détection d'objets. Restera encore la partie de l'interprétation des dangers potentiels d'un objet et là, il y a encore du chemin à* ●●●

PAROLE DE JURISTE

ANTHONY COQUER

Directeur du département Sécurité et organisation chez Alain Bensoussan-Avocats

© DR

« GARDER À L'ESPRIT LA FINALITÉ PREMIÈRE DES INSTALLATIONS ET DES DONNÉES COLLECTÉES. »

« On ne peut pas faire n'importe quoi avec les données. C'est-à-dire toutes les traces que nous laissons sur les réseaux sociaux, ou avec nos téléphones, ou sur les séquences enregistrées par des installation de vidéosurveillance. Alors, certes, on peut comprendre que lorsqu'un organisme, une entreprise, un service de l'État… collecte des informations, c'est qu'il souhaite s'en servir. Mais il faut que cette collecte des informations et leur utilisation se fasse de manière loyale et transparente. Le problème se pose particulièrement avec les caméras de vidéosurveillance qui sont de plus en plus intelligentes et qui sont désormais capables de reconnaître des formes, de détecter des colis suspects, d'identifier des personnes, de remonter – via le suivi d'un individu – vers d'autres traitements qui permettent d'identifier cet individu… L'utilisation des métadonnées pose donc quelques problèmes. Il faut garder à l'esprit la finalité des installation et se garder d'associer différentes sources de données ayant des finalités différentes. »

2 QUESTIONS À

FRANÇOIS PERRACHON

Senior VP Global Sales, Public Security chez Idemia

© DR

Quelles sont les solutions proposées par Idemia en matière d'exploitation des métadonnées ?

Les solutions d'Idemia dans le domaine de l'analyse de vidéo et de photo visent essentiellement à ajouter des métadonnées de contenu – celles qui décrivent la vidéo ou la photo – sur des données qui n'en contiennent pas initialement. Il s'agit donc par exemple de dire : « Cette vidéo, tournée à tel endroit et entre 17 heures et 19 h 32, contient à 17 h 23 une petite voiture rouge immatriculée AA 111 ZZ, conduite par une dame jeune à lunettes » et « Ces deux photos, toutes les deux saisies dans le cadre d'une enquête de pédopornographie, montrent chacune un bras adulte avec le même tatouage » et de compléter avec « Sur les vidéos de surveillance de cette ville, à la suite de la plainte d'une dame qui dit être suivie tous les soirs par un individu lorsqu'elle rentre chez elle, on trouve bien la dame en question sur plusieurs caméras à travers la ville, et on voit effectivement qu'elle est suivie toujours par le même homme. » Les solutions vidéo d'Idemia consistent donc à ajouter des métadonnées de contenu aux vidéos et aux photos saisies dans le cadre d'enquêtes, à les rajouter aux métadonnées de contexte (lieu, date, etc.) et à permettre à un enquêteur d'utiliser toutes ces données pour analyser très rapidement les données image saisies.

Pouvez-vous nous donner un exemple concret d'utilisation des métadonnées à des fins sécuritaires ?

En voici un, tout à fait parlant. Après une tentative d'homicide dans un lieu public, un homme est interpellé : il n'y a aucun doute qu'il soit l'auteur de la tentative d'homicide, cependant il est nécessaire de déterminer s'il y a eu ou non préméditation. Pour répondre à cette question, la police saisit des vidéos enregistrées avant la tentative d'homicide : cela correspond à plusieurs jours d'enregistrement sur six caméras. Il s'agit de déterminer si l'homme interpellé est visible sur ces enregistrements, et au cas où il l'est, s'il fait du repérage. Regarder l'intégralité de ces heures de vidéos séquentiellement représenterait un travail colossal. Par ailleurs, s'agissant d'un lieu où il y a beaucoup de monde, il serait très difficile et fatigant de parvenir à identifier un individu parmi la foule « rien qu'avec ses yeux ».
Grâce à une photo de l'homme interpellé, prélevée sur son téléphone portable, les vidéos analysées automatiquement par le produit Idemia sont exploitées très rapidement. On recherche le visage de l'homme interpellé sur la collection des visages extraite des vidéos, et on constate s'il apparaît ou pas.
En l'occurrence, il y était. Les courtes séquences vidéo où l'homme a été vu ont pu facilement être extraites et versées au dossier de cette enquête.

3 QUESTIONS À

PATRICK DUVERGER

Responsable des systèmes d'information et moyens généraux, Ville d'Antibes

© DR

Comment la Ville d'Antibes en est-elle venue à envisager d'utiliser les métadonnées, le deep learning… pour optimiser l'utilisation de son réseau de 165 caméras de vidéosurveillance ?

Nous sommes partis d'un constat technique assez simple. Tout d'abord, la vidéoprotection a réussi à s'imposer comme une solution efficace pour aider les forces de police. En raison de cette généralisation de la vidéoprotection, les villes ont bénéficié d'importantes évolutions technologiques : des caméras de plus en plus précises et perfectionnées, un réseau les reliant au central en très haut débit, des centres de supervision urbains avec derrière la scène des serveurs plus puissants. Tout cela constitue un « patrimoine » numérique qui peut être mieux exploité par la ville. En outre, sous l'impulsion de Jean Leonetti, nous sommes, depuis plusieurs années, très impliqués dans une démarche de smart city pour rendre la ville plus intelligente via une roadmap précise. La roadmap de Smart Antibes est organisée selon trois pôles : l'internet des objets, l'internet des personnes et l'internet des services publics. Il s'agit d'interconnecter les capteurs de la ville avec les services publics que l'on souhaite développer et numériser davantage pour répondre à la demande citoyenne. Si nous avons déjà mené des partenariats pour développer l'internet des objets, nous nous sommes dits qu'au lieu de rajouter des capteurs dans la ville, nous pouvions récupérer les informations de capteurs déjà en place : les caméras de vidéosurveillance. Tous ces capteurs qui regardent la ville peuvent nous aider à prendre le pouls de l'agglomération. Pour analyser les flux de véhicules et de personnes qui circulent, pour analyser le trafic, réduire les dépenses d'éclairage public (l'éclairage augmente si des piétons sont détectés), lever une alerte si un utilitaire suspect est proche d'une école, etc.

Comment passe-t-on d'une simple caméra à une caméra capteur ?

L'enjeu du projet que nous menons avec SAP, Digital Barriers et Nvidia, réside dans notre capacité à transformer une caméra de vidéosurveillance en un capteur de la smart city. En une phrase : comment passer de la « safe city » à la « smart city » ? Ou comment transformer un flux vidéo en capteur intelligent ? Il s'agit de passer d'une image à une information analytique, c'est-à-dire une information alphanumérique : du texte et des chiffres, embouteillage ou pas, nombre de véhicules, nombre de piétons, anomalie ou danger ? Voilà le type d'information que l'on veut collecter de manière silencieuse et automatique. Pour parvenir à faire cela, il faut une analyse intelligente et automatique de la vidéo. Dans ce projet, nous mettons les algorithmes d'intelligence artificielle au service de la gestion de la cité.

Vous travaillez donc à la mise en pratique des fameux réseaux neuronaux ?

Tout à fait. Avec l'évolution de la puissance des microprocesseurs et surtout avec l'utilisation des capacités de calculs massivement parallèles des cartes graphiques, l'implémentation des réseaux neuronaux est passée de la théorie à la pratique. C'est pour cela que nous avons NVidia comme partenaire : ils nous fournissent la puissance de calcul des cartes graphiques (puissance que l'on appelle GPU). De son côté, Digital Barriers nous donne l'expertise pour développer les réseaux neuronaux qui vont s'exécuter en aval du flux vidéo de la caméra pour détecter les véhicules, les personnes, les objets, et nous fournir en temps réel une masse gigantesque d'informations sur l'activité de la ville. Enfin SAP, 1er éditeur de logiciels d'Europe, avec lequel nous avons une longue histoire de partenariat, fournit la puissance de traitement de toutes ses informations avec la base de données en mémoire Hana et la suite logicielle Leonardo pour l'IOT que nous allons utiliser sur un type de capteur un peu exotique : des caméras rendues intelligentes grâce aux réseaux neuronaux de Digital Barriers. Toutes ces briques vont nous permettre d'indexer la ville, passer d'une information type image ou vidéo qui est destinée à être regardée par un opérateur, à une information analytique textuelle pouvant être stockée dans des bases de données, faire des analyses statistiques, lever des alertes, calculer des fréquentations, etc. En d'autres termes, nous allons convertir le flux vidéo en de l'information qualifiée pour utiliser la puissance de la Business Intelligence de SAP, et offrir à la fin du projet un moteur d'aide à la décision pour la gestion de Smart Antibes. Notre objectif est d'utiliser au maximum ces formidables outils pour ajouter à la vidéoprotection des fonctionnalités de supervision de la cité.

● ● ● *faire. Ne pas oublier que l'interprétation est souvent contextuelle et que les machines devront de plus en plus apprendre à interpréter un contexte. »*

Du côté de la loi, il faut tout de même se poser certaines questions. Ce que n'hésite pas à faire Anthony Coquer, directeur du département Sécurité et organisation chez Alain Bensoussan-Avocats : *« Nous vivons dans un monde où nous générons tous un nombre très important de traces, sans en avoir toujours conscience. Loin de là. Et le législateur l'a compris, tout comme l'Union européenne, en décidant de mettre en place le RGPD qui entrera en vigueur le 25 mai de cette année. Il sera complété par un important volet qui viendra renforcer les obligations sur les métadonnées et les empreintes numériques. Certes, on ne peut pas empêcher les outils électroniques de collecter des traces, des images, des empreintes, des données… et il est tentant de les utiliser pour une multitude de fins. Qu'elles soient sécuritaires ou autres. Mais, attention, dans le cas des métadonnées utilisées dans la sécurité, il faut garder à l'esprit que cela ne peut se faire en dehors des fins premières de l'installation : pour de la sécurité. Et d'autre part, que les données utilisées à des fins de sécurité n'ont pas été collectées en tout premier lieu pour d'autres finalités n'ayant rien à voir avec la sécurité. Ce qui poserait la question de la légitimité de leur utilisation. Et serait sans doute sanctionné par la justice. »* ■