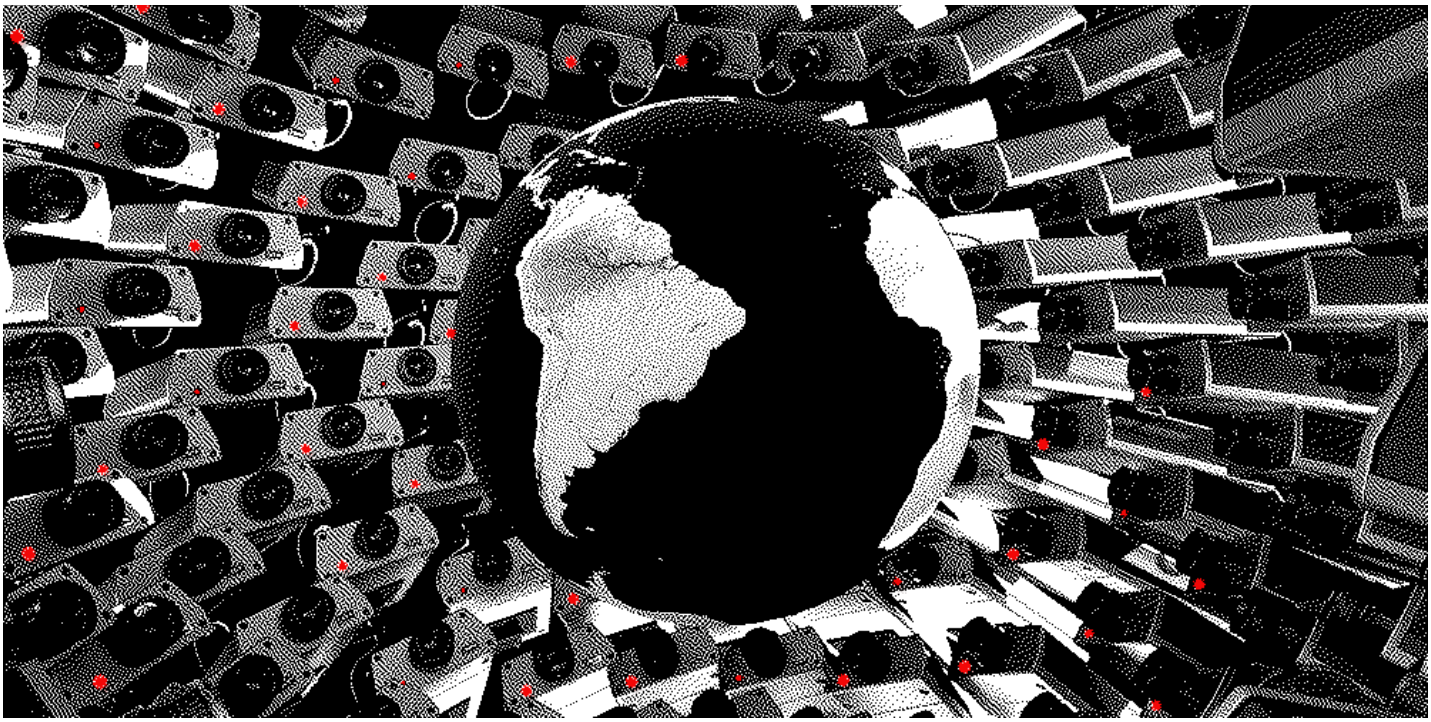
L'ESSOR DES RÉSEAUX DE CAMÉRAS INTELLIGENTES, À BANNIR ? VOILA POURQUOI

27 janvier 2020 Par Michael Kwet https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/



LA RECONNAISSANCE FACIALE INQUIETE UN PEU PARTOUT.
Qu'on puisse, par caméra, suivre nos moindres mouvements en public préoccupe beaucoup plus que l'existence et la prévalence exponentielle des réseaux de vidéosurveillance intelligents", alors qu'il s'agit d'un sujet tout aussi inquiétant.

Les ménages et les sociétés privées commencent à connecter leurs caméras sur les réseaux policiers, et les rapides progrès de l'intelligence artificielle donnent aux réseaux de télévision en circuit fermé le pouvoir de surveiller la totalité de l'espace public. Dans un avenir pas si lointain, nos forces de police, nos magasins, et notre administration municipale espèrent pouvoir filmer notre moindre mouvement, et même mieux, l'interpréter par le biais de l'analyse des métadonnées.

L'émergence de la caméra intelligente à vision panoramique n'est pas à prendre à la légère. Elle menace les droits et les libertés des citoyens du monde entier. Voilà longtemps que la surveillance est utilisée par les forces de l'ordre à l'encontre des communautés marginalisées, et la recherche indique qu'elle restreint la liberté d'expression -- ces effets pervers ne vont qu'empirer alors que les réseaux de vidéosurveillance gagnent en taille et en sophistication.

Pour comprendre ce qu'il se passe, il faut comprendre l'essor du complexe industriel de la vidéosurveillance -- son histoire, ses puissants protagonistes, et ses perspectives d'avenir. Il est né avec la prolifération des caméras de police et de sécurité, et aboutit à un nouvel impératif industriel majeur: la surveillance visuelle intégrale de l'espace public.

Systèmes de gestion vidéo (SGV) et maillages de réseaux de surveillance extensibles [Plug-in networks]
Durant les premières décennies de leur existence, les télévisions en circuit fermé étaient des outils analogiques à basse résolution, enregistrant sur des bandes. Des entreprises et des autorités publiques les employaient pour filmer de petites zones précises. Elles étaient peu nombreuses dans l'espace public, et la

possibilité de suivre des individus était limitée. Pour poursuivre une personne en particulier, la police devait passer des heures afin d'aller à pied récupérer les données des caméras environnantes.

Vers la fin des années 1990, la vidéosurveillance a fait un grand bond en avant. Axis Communication a mis au point la première caméra de surveillance connectée, capable de transformer des vidéos en données numériques. De nouvelles entreprises, telles Milestone Systems, ont élaboré des systèmes de gestion vidéo, ou SGV, pour compiler les informations dans des bases de données. Ces prestataires SGV y ajoutèrent des fonctions comme le détecteur de mouvement, capables d'alerter les vigiles si une personne pénétrait dans une zone réglementée.

Au fil du temps, la surveillance vidéo s'est répandue. A un moment donné, il y a près de 50 ans, le Royaume-Uni avait quelque chose comme 60 caméras de surveillance permanente dans le pays. Aujourd'hui il en compte plus de six millions, tandis que les États-Unis en ont des dizaines de millions. Selon IHS Markit, une société de marketing, plus d'un milliard de caméras surveilleront le monde d'ici fin 2021, et les États-Unis rivaliseront avec la Chine en termes de taux de pénétration de caméras par personne. La police peut désormais, au fil de multiples caméras, à partir d'un centre de commande et contrôle, traquer des individus sur un PC ou même un smartphone.

Bien qu'il soit possible de relier des milliers de caméras par un SGV, c'est cependant coûteux. Pour récupérer encore plus de données, les administrations ont trouvé un nouveau truc intelligent: encourager les entreprises et les particuliers à connecter leurs caméras privées aux réseaux des forces de l'ordre -- ce que j'appelle "maillage de réseaux de surveillance extensibles".

Les vidéos des caméras de surveillance de la ville sont diffusées au Real-Time Crime Center, l'espace de visualisation du projet Green Light, au quartier général de la police de Detroit, le 14 juin 2019. Photo : Brittany Greeson/The New York Times via Redux

En regroupant les caméras municipales d'une ville et les caméras privées, les experts de la police affirment qu'une agence dans une grande ville typique peut, en quelques années seulement, recueillir des centaines de milliers de flux vidéo.

C'est au travers de son programme polémique, le projet Green Light,que Detroit a popularisé son maillage de réseaux, il permet aux entreprises d'acheter des caméras en circuit fermé et de les connecter aux commissariats de la ville.

Elles peuvent aussi placer un point lumineux vert près de leur dispositif pour indiquer qu'elles font partie du réseau de police. Le projet affirme ainsi dissuader les criminels en rappelant aux citoyens : La police vous observe.

Il ne s'agit pas seulement de Detroit. Chicago, la Nouvelle Orléans, New York et Atlanta ont elles aussi déployé leurs propres maillages de réseaux de surveillance extensibles. Dans ces villes, tant les entreprises que les ménages fournissent des flux aux forces anti-criminalité ce qui permet à la police d'accéder aux images en temps réel mais aussi aux enregistrements. La police de New Haven, dans le Connecticut, m'a dit s'intéresser au même système, et elle n'est sûrement pas la seule.

Le nombre de caméras sur les réseaux de police varie aujourd'hui de plusieurs dizaines de milliers (Chicago) à plusieurs centaines (Nouvelle-Orléans). Avec autant de caméras en place, et seulement une petite équipe d'agents pour les surveiller, les services de police sont confrontés à un nouveau défi : comment donner un sens à toutes ces images ? La réponse se trouve dans la lecture analytique.

L'essor de la lecture analytique
En 2006, une jeune Israélienne enregistrait des vidéos de famille chaque week-end, mais étudiante et mère de famille, elle n'avait pas le temps de les regarder. Shmuel Peleg, professeur en informatique de son université, m'a expliqué avoir cherché une solution pour elle : il voulait partir d'une longue vidéo pour en extraire les moments intéressants, condensés en un clip video. Son système n'a pas fonctionné : cela requérait des caméras statiques or celle de son élève se déplaçait quand elle filmait sa famille.

Peleg a cependant rapidement trouvé un autre débouché dans l'industrie de la vidéosurveillance, qui s'appuie sur des dispositifs statiques. Son invention est devenue BriefCam, une entreprise de lecture analytique qui peut condenser les séquences vidéos d'une scène à travers le temps afin que les enquêteurs puissent en visionner tous les moments pertinents en un temps très bref.

// VIDEO https://youtu.be/lOnZ_E71sY4

Grâce à une fonction appelée Video Synopsis, BriefCam superpose des images d'événements se produisant à différents moments comme s'ils apparaissaient simultanément. Par exemple, si plusieurs personnes sont passées devant une caméra à 12h30, 12h40 et 12h50, BriefCam regroupera leurs images en une seule scène.

Les enquêteurs peuvent visionner toutes les séquences intéressantes d'une journée donnée en quelques minutes au lieu de devoir y passer plusieurs heures. Grâce aux progrès rapides de l'intelligence artificielle, cette fonction de résumé n'est qu'une des caractéristiques de la gamme de produits BriefCam et de l'industrie de l'analyse vidéo en pleine expansion.

La reconnaissance du comportement intègre des capacités d'analyse vidéo telles que la détection des bagarres, la reconnaissance des émotions, la détection des chutes, la flânerie, la promenade des chiens, la traversée en dehors des passages piétons, la fraude au péage et même la détection de mensonges. La reconnaissance d'objets permet de reconnaître des visages, des animaux, des voitures, des armes, des feux et bien d'autres choses encore, ainsi que des caractéristiques humaines comme le sexe, l'âge et la couleur des cheveux.

La détection de comportements anormaux ou inhabituels fonctionne en enregistrant une zone fixe pendant une période de temps - disons 30 jours - et en déterminant le comportement "normal" pour cette scène. Si la caméra voit quelque chose d'inhabituel - par exemple, une personne qui court dans une rue à 3 heures du matin - elle signale l'incident pour attirer l'attention.

Les systèmes analytiques vidéo peuvent analyser et fouiller des flux en temps réel ou des séquences enregistrées. Ils peuvent également isoler des individus ou des objets lorsque ces derniers pénètrent dans un réseau de caméras intelligentes. Chicago; la Nouvelle-Orléans; Detroit; Springfield, Massachusetts; et Hartford, Connecticut, sont quelques-unes des villes qui utilisent actuellement BriefCam pour le maintien de l'ordre.

Effectuer des recherches, mener des enquêtes
Les espaces urbains étant truffés de caméras, et l'analyse vidéo permettant de leur donner un sens, les forces de l'ordre ont la possibilité de tout enregistrer et de tout analyser, tout le temps. Cela donne aux autorités le pouvoir d'indexer et de rechercher dans une vaste base de données d'objets, de comportements et d'activités anormales.

Dans le Connecticut, la police a utilisé l'analyse vidéo pour identifier ou surveiller des trafiquants de drogue avérés ou suspectés. Le sergent Johnmichael O'Hare, ancien directeur du Hartford Real-Time Crime Center, a récemment démontré comment BriefCam a aidé la police de Hartford à révéler "où les gens vont le plus" en l'espace de 24 heures en visionnant des images condensées et résumées en seulement neuf minutes. En utilisant une fonction appelée "pathways", il a découvert des centaines de personnes visitant seulement deux maisons dans la rue et a obtenu un mandat de perquisition pour vérifier qu'il s'agissait bien de maisons de la drogue.

La start-up d'analyse vidéo Voxel51 ajoute également des fonctions de recherche plus sophistiquées. Co-fondée par Jason Corso, professeur d'ingénierie électrique et d'informatique à l'université du Michigan, la société offre une plateforme de traitement et de d'analyse vidéo.

Corso m'a dit que sa société espère offrir le premier système où les gens peuvent "faire des recherches basées sur le contenu sémantique de leurs données, comme par exemple, 'Je veux trouver tous les clips vidéo qui ont plus de trois intersections ... avec au moins 20 véhicules pendant la journée'". Voxel51 "essaie de rendre cela possible" en prenant des séquences vidéo et en les "transformant en données de recherche structurées sur différents types de plateformes".

A la différence de BriefCam, qui analyse la vidéo en n'utilisant que son propre logiciel, Voxel51 offre une plateforme ouverte qui permet à des tiers d'ajouter leurs propres modèles d'analyse. Si la plateforme réussit, elle augmentera la capacité de recherche et de surveillance des espaces publics.

Corso m'a aussi précisé que sa société travaille sur un projet pilote avec la police de Baltimore concernant leur programme de surveillance CitiWatch et prévoit de tester le logiciel avec le département de police de Houston.

Alors que les villes commencent à déployer un vaste éventail de dispositifs de surveillance à partir de ce qu'on appelle l'Internet des objets, les chercheurs développent également une technique connue sous le nom d'analyse vidéo et de fusion de données de capteurs, ou VA/SF, pour le service de renseignements de la police. Avec la VA/SF, de multiples flux provenant de capteurs sont combinés avec l'analyse vidéo afin de réduire les imprécisions et de faire des déductions à propos de situations complexes. Par exemple, Peleg m'a dit que BriefCam développe une analyse audio à partir d'une caméra qui utilise des microphones pour détecter les actions qui peuvent perturber les systèmes d'IA, par exemple distinguer si des gens se battent ou dansent.

Les PMV [Les panneaux à messages variables, panneaux de signalisation routière conçus pour alerter ou informer l'usager de la route;NdT] offrent également une intégration intelligente entre les différentes technologies. L'ancien chef de la police de New Haven, Anthony Campbell, m'a raconté comment les ShotSpotters, des appareils controversés qui écoutent les coups de feu, s'intègrent à des logiciels spécialisés de sorte que lorsqu'un coup de feu est tiré, les caméras pivotantes situées à proximité modifient instantanément leur direction en fonction de l'endroit où l'arme a été tirée.

Les agents peuvent également utiliser un logiciel pour verrouiller les portes des bâtiments à partir d'un centre de contrôle, et les entreprises développent des analyses pour alerter la sécurité si une voiture est suivie par une autre.

Vers un monde digne de "Minority Report"
[En 2054, la société du futur a éradiqué les crimes en se dotant d'un système de prévention, détection et répression le plus sophistiqué du monde;NdT] L'analyse vidéo capte une grande variété de données sur les zones couvertes par les réseaux de caméras intelligentes. Il n'est pas surprenant que les informations recueillies soient maintenant proposées dans le cadre de la police prédictive : l'utilisation de données pour prévoir et contrôler la criminalité avant qu'elle ne se produise.

En 2002, le film dystopique "Minority Report" a dépeint une société utilisant l'analyse "pré-crime" pour permettre à la police d'intervenir en cas d'infraction à la loi bien avant que celle-ci ne se produise. Finalement, les officiers responsables en viennent à tenter de manipuler le système à leurs propres fins.

Une version authentique de " Minority Report " est en train de voir le jour dans le vrai monde par le biais de centres de criminalité qui analysent, pour la police et en temps réel les modèles de criminalité. Dans ces centres, les forces de l'ordre ingèrent des informations provenant de sources telles que les réseaux de médias sociaux, les fournisseurs de données, les bases de données publiques, les casiers judiciaires et les ShotSpotters. Les données météorologiques y sont même introduites pour leur impact sur la criminalité (car, c'est bien connu, "les méchants n'aiment pas la pluie").

Dans un document datant de 2018, la société de gestion de données Western Digital et le cabinet de conseil Accenture ont annoncé que des réseaux de caméras intelligentes de masse seraient déployés " selon trois niveaux de maturité ". Cette adoption en plusieurs étapes, ont-ils affirmé, "permettrait à la société" d'abandonner progressivement "les préoccupations relatives à la vie privée" et même au contraire "d'accepter et de prôner" la surveillance policière et gouvernementale de masse dans l'intérêt de la "sécurité publique".

Le niveau 1 englobe le stade actuel où la police utilise les réseaux de CCTV pour enquêter sur les crimes après coup. D'ici 2025, la société atteindra le niveau 2 au fur et à mesure que les municipalités se transformeront en villes "intelligentes", indique le document. Les entreprises et les institutions publiques, tout comme les écoles et les hôpitaux, raccorderont des caméras aux agences gouvernementales et policières afin d'alimenter des systèmes d'analyse centralisés et basés sur l'intelligence artificielle.

Au niveau 3 qui arrivera d'ici 2035, le système de surveillance sera le plus prédictif, . Certains résidents feront volontairement don des images de leurs caméras, tandis que d'autres seront "encouragés à le faire par des incitations fiscales ou une compensation nominale". Un "écosystème de sécurité publique" centralisera les données "tirées de bases de données disparates telles que les médias sociaux, les permis de conduire, les bases de données de la police et les données collectées mais non exploitées [Dark data; NdT]". Une unité d'analyse basée sur l'IA permettra à la police d'évaluer "les anomalies en temps réel et d'interrompre un crime avant qu'il ne soit commis". Autrement dit, intercepter les pré-crimes.

L'essor du complexe industriel de la vidéosurveillance

Alors que la surveillance par CCTV a commencé comme un simple outil de justice pénale, elle est devenue une industrie valant plusieurs milliards de dollars qui couvre plusieurs secteurs verticaux. Depuis le maintien de l'ordre et les villes intelligentes jusqu'aux écoles, aux établissements de soins de santé et aux commerces de détail, la société se dirige vers une surveillance vidéo quasi intégrale des espaces commerciaux et urbains. La société danoise Milestone Systems, l'un des principaux fournisseurs de PMV, dont la moitié des revenus provient des États-Unis, comptait moins de 10 employés en 1999. Il s'agit aujourd'hui d'une grande entreprise qui revendique des bureaux dans plus de 20 pays.

Axis Communications était à l'origine un fabricant d'imprimantes réseau. Depuis, cette entreprise est devenue l'un des principaux fournisseurs de caméras, avec un chiffre d'affaires annuel de plus d'un milliard de dollars. BriefCam a démarré comme un projet universitaire. Actuellement, cette entreprise figure parmi les meilleurs fournisseurs d'analyse vidéo au monde, avec des clients dans plus de 40 pays.

Au cours des six dernières années, Canon a acheté les trois, donnant au conglomérat de l'imagerie la mainmise sur des géants de l'industrie dans le domaine des logiciels de gestion vidéo, des caméras de surveillance et de l'analyse vidéo. Motorola a récemment acquis un des principaux fournisseurs de PMV, Avigilon, pour un milliard de dollars. À leur tour, Avigilon et d'autres grandes entreprises ont acheté leurs propres sociétés.

Le public paie trois fois pour sa propre surveillance de haute technologie.

Des géants de la technologie bien connus sont également de la partie. Le lieutenant Patrick O'Donnell, des forces de police de Chicago, m'a dit que son département travaillait sur un accord de non-divulgation avec Google pour un projet pilote d'analyse vidéo visant à détecter les personnes réagissant à des tirs d'armes à feu, et si elles sont en position couchée, afin que la police puisse recevoir des alertes en temps réel. (Google n'a pas répondu à une demande de commentaires).

Les réseaux de vidéosurveillance impliquent inévitablement tout un écosystème de fournisseurs, dont certains ont offert, ou pourraient encore offrir, des services spécifiquement destinés à ces systèmes. Microsoft, Amazon, IBM, Comcast, Verizon et Cisco sont parmi ceux qui permettent aux réseaux de fonctionner avec des technologies telles que les services en cloud, la connectivité à large bande ou les logiciels de vidéosurveillance.

Dans le secteur public, le National Institute of Standards and Technology finance des "analyses publiques" et des réseaux de communication comme le First Responder Network Authority, ou FirstNet, pour la vidéo en temps réel et autres technologies de surveillance. FirstNet, construit par AT&T, coûtera 46,5 milliards de dollars.

Voxel51 est également une entreprise soutenue par le NIST. Le public paie donc trois fois sa propre surveillance de haute technologie : premièrement, par le biais de taxes pour la recherche universitaire ; deuxièmement, par le biais de subventions pour la création d'une start-up à but lucratif (Voxel51) ; et troisièmement, par l'achat des services de Voxel51 par les services de police de la ville qui utilisent des fonds publics.

Les secteurs privé et public cherchant à étendre la présence des caméras, la vidéosurveillance est devenue une nouvelle vache à lait. Comme le dit Corso, "il y aura quelque chose comme 45 milliards de caméras dans le monde d'ici quelques décennies. Cela fait beaucoup de pixels (vidéo). La majeure partie de ces pixels restent inexploités". L'estimation de Corso reflète les prévisions de la société de capital-risque new-yorkaise LDV pour 2017, celle-ci pense que les smartphones évolueront pour avoir encore plus de caméras qu'aujourd'hui, contribuant ainsi à cette croissance.

Les entreprises qui ont commencé par les marchés de la police et de la sécurité diversifient maintenant leurs offres vers le secteur commercial. BriefCam, Milestone et Axis font la promotion de l'utilisation de l'analyse vidéo pour les détaillants, qui peuvent ainsi surveiller la circulation des piétons, la longueur des files d'attente, les habitudes d'achat, la disposition des rayons et effectuer des tests A/B [Le test A/B est une technique de marketing qui consiste à proposer plusieurs variantes d'un même objet qui diffèrent selon un seul critère afin de déterminer la version qui donne les meilleurs résultats auprès des consommateurs;NdT]. Voxel51 a une option conçue pour l'industrie de la mode et prévoit de se développer dans les secteurs verticaux de l'industrie. Motionloft propose des analyses pour les villes intelligentes, les détaillants, l'immobilier commercial et les lieux de divertissement. D'autres exemples abondent.

Les acteurs des secteurs public et privé font pression en faveur d'un monde truffé de vidéosurveillance intelligente. Peleg, par exemple, m'a parlé d'un exemple de villes intelligentes : Si vous entrez en ville en voiture, vous pourriez "juste vous garer et rentrer chez vous" sans utiliser de parcmètre. La ville enverrait une facture à votre domicile à la fin du mois. "Bien sûr, vous renoncez à votre vie privée", a-t-il ajouté. "La question est de savoir si vous tenez vraiment à ce que Big Brother sache où vous êtes, ce que vous faites, etc. Certaines personnes peuvent ne pas aimer ça".

Comment tenir en laisse la surveillance intelligente

Ceux qui n'aiment pas ces nouvelles formes de surveillance "Big Brother" se focalisent actuellement sur la reconnaissance faciale. Pourtant, ils ont largement ignoré le passage aux réseaux de caméras intelligentes - et le complexe industriel qui le sous-tend.

Des milliers de caméras sont désormais installées pour surveiller chacun de nos mouvements, informant les autorités municipales si nous marchons, courrons, faisons du vélo ou faisons quoi que ce soit de "suspect". Avec l'analyse vidéo, l'intelligence artificielle est utilisée pour identifier notre sexe, notre âge et notre type de vêtements, et pourrait éventuellement être utilisée pour nous classer par race ou par tenue religieuse.

Une pareille surveillance pourrait avoir un effet paralysant considérable sur notre liberté d'expression et d'association. Est-ce là le monde dans lequel nous voulons vivre ?

La possibilité de suivre des personnes sur des réseaux de télévision en circuit fermé intelligents peut être utilisée pour cibler les communautés marginalisées. La détection de la " flânerie " ou du " vol à l'étalage " par des caméras concentrées dans les quartiers pauvres peut aggraver les préjugés raciaux des pratiques

policières. On constate déjà ce type de discrimination raciale en Afrique du Sud, où la "détection des comportements inhabituels" est déployée depuis plusieurs années par des réseaux de caméras intelligentes.

Aux États-Unis, les réseaux de caméras intelligentes sont en train d'émerger, et il y a peu d'informations ou de transparence quant à leur utilisation. Néanmoins, nous savons que la surveillance a été utilisée tout au long de l'histoire pour cibler les groupes opprimés. Ces dernières années, la police de New York a secrètement espionné les musulmans, le FBI a utilisé des avions de surveillance pour suivre les manifestants de Black Lives Matter, et le service américain des douanes et de la protection des frontières a commencé à construire une "frontière intelligente" de surveillance vidéo de haute technologie à travers la réserve de la tribu Tohono O'odham en Arizona.

Les forces de l'ordre prétendent que les réseaux de caméras intelligentes réduiront la criminalité, mais à quel prix ? Si une caméra pouvait être installée dans chaque pièce de chaque maison, la violence domestique pourrait diminuer. Nous pourrions ajouter des "filtres" automatiques qui n'enregistrent que lorsqu'un bruit fort est détecté, ou lorsque quelqu'un saisit un couteau. La police devrait-elle installer des caméras intelligentes dans chaque salon ?

Le secteur commercial rationalise également l'avancée du capitalisme de surveillance dans le domaine physique. Les détaillants, les employeurs et les investisseurs veulent tous nous placer sous surveillance vidéo intelligente afin de pouvoir nous gérer avec une "intelligence" visuelle.

Interrogés sur le respect de la vie privée, plusieurs départements de police importants m'ont dit qu'ils avaient le droit de voir et d'enregistrer tout ce que vous faites dès que vous quittez votre domicile. Les revendeurs de ces systèmes, quant à eux, ne cherchent même pas à divulguer des informations au public : ils gardent secrètes leurs pratiques d'analyse vidéo.

Aux États-Unis, il n'existe pas d'"attente raisonnable" concernant le respect de la vie privée en public. Le quatrième amendement (de la Constitution, NdT) protège les foyers et certains espacespublics pouvant "raisonnablement" être considérés comme privés, à l'instar d'une cabine téléphonique. A peu près partout ailleurs - dans nos rues, nos magasins ou nos écoles - tout est permis.

Même si des lois sont votées pour encadrer l'utilisation de la vidéosurveillance, nous ne pouvons pas garantir qu'elles resteront en vigueur pour toujours. Avec des milliers de caméras haute résolution mises en réseau, un état de surveillance dystopique est à un clic de souris. En installant des caméras partout, nous ouvrons une boîte de Pandore.

Pour répondre aux menaces que font peser sur notre vie privée ces réseaux de caméras intelligentes, les législateurs devraient interdire les maillages de réseaux de surveillance extensibles et limiter la portée des caméras en circuit fermé à un seul site. La densité des caméras et des capteurs dans l'espace public devrait aussi être restreinte. La possibilité de suivre des individus sur une longue distance serait donc impossible, et empêcherait ce phénomène de surveillance permanente.

Le gouvernement devrait aussi interdire la lecture analytique de la vidéosurveillance dans les espaces publics, moyennant peut-être des exceptions spécifiques comme la détection de corps sur les voies ferrées. Une telle interdiction découragerait les déploiements en masse de ces dispositifs, car la lecture analytique est le seul moyen pour d'exploiter des volumes d'enregistrements aussi importants. Les tribunaux devraient d'urgence reconsidérer la portée du quatrième amendement et étendre notre droit au respect de la vie privée dans l'espace public.

Les services de police, leurs fournisseurs et les chercheurs doivent publier leurs résultats, et discuter ouvertement avec les universitaires, les journalistes, et la société civile.

Il est évident que nous assistons ici aux prémices d'une crise. Il faut dépasser le débat simpliste autour de la reconnaissance faciale et s'attaquer au problème beaucoup plus large de la vidéosurveillance, avant qu'il ne soit trop tard.